



**RAT DER
EUROPÄISCHEN UNION**

**Brüssel, den 25. November 2009 (26.11)
(OR. en)**

16637/09

**JAI 873
CATS 131
ASIM 137
JUSTCIV 249
JURINFO 145**

I/A-PUNKT-VERMERK

des Generalsekretariats
für den AStV/Rat

Nr. Vordokument: 15857/09 JAI 825 CATS 121 ASIM 127 JUSTCIV 237 JURINFO 142

Betr.: Entwurf von Schlussfolgerungen des Rates zu einer Strategie für das Informationsmanagement im Bereich der inneren Sicherheit in der EU

1. Der Vorsitz hat der Ad-hoc-Gruppe "Informationsaustausch" am 16. Juni 2009 einen Vorschlag für eine Strategie für das Informationsmanagement vorgelegt. Mit dieser Strategie soll nicht bestimmt werden, welche Art von Informationen zu speichern und/oder auszutauschen sind, sondern sie stellt vielmehr eine Methode (das "Wie") bereit, mit der sichergestellt werden soll, dass Entscheidungen über die Notwendigkeit der Verarbeitung und des Austauschs von Daten und Entscheidungen über die entsprechenden Mittel und Wege in kohärenter, professioneller, effizienter und kostenwirksamer Weise getroffen werden und gleichzeitig der Rechenschaftspflicht gegenüber Bürgern und beruflichen Nutzern Genüge geleistet wird und die Entscheidungen für diese durchschaubar bleiben. Es ist kein rechtsverbindlicher Text. In Verbindung mit den Prioritäten der EU im Bereich Justiz und Inneres – insbesondere in Bezug auf die innere Sicherheit¹ (das "Was") – wird es die Strategie für das Informationsmanagement den zuständigen Behörden ermöglichen, künftige Entwicklungen beim grundsätzlichen Vorgehen im Bereich des Informationsaustauschs effizient und effektiv umzusetzen.

¹ Ein Mitgliedstaat kann beschließen, diese Strategie mittels eines schrittweisen Konzepts anzuwenden, indem beispielsweise die Anwendung auf spezifische Bereiche der inneren Sicherheit wie etwa Strafverfolgung und justizielle Zusammenarbeit in Strafsachen beschränkt wird. Gelangt dieser Mitgliedstaat aufgrund seiner Erfahrungen zu der Auffassung, dass das Konzept dieser Strategie auch auf andere Bereiche angewandt werden sollte, kann er beschließen, die Anwendung auszuweiten.

2. Die Strategie stellt das Grundlagenpapier dar und ist in dieser Funktion langfristig angelegt. Sie kann entsprechend der Fortentwicklung und Änderung der übergeordneten Zielvorstellungen weiterentwickelt und aktualisiert werden und sollte bis Ende 2014 überprüft werden. Die Strategie für das Informationsmanagement wird durch einen Maßnahmenkatalog/Fahrplan, in dem die konkreten Ziele, Verfahren, Aufgaben und Fristen festgelegt werden, ergänzt werden.
3. Die Ad-hoc-Gruppe "Informationsaustausch" hat den Vorschlag in ihren Sitzungen vom 7. und 13. Juli, 26./27. September sowie 15. und 26. Oktober eingehend erörtert und abgesehen von einigen Vorbehalten zu der Tragweite des Dokuments eine allgemeine Einigung über den Text erzielt. Der Ausschuss "Artikel 36" hat den Vorschlag in seiner Sitzung vom 10./11. November 2009 erörtert und, abgesehen von den Vorbehalten von CZ, DE, AT und LT, eine Einigung über den Entwurf von Schlussfolgerungen erzielt.
4. Der AStV hat den Entwurf von Schlussfolgerungen auf seiner Tagung vom 20. November 2009 erörtert und die betreffenden Delegationen gebeten, ihre Vorbehalte zurückzuziehen. Diese Vorbehalte wurden im Anschluss an die Tagung aufgehoben.
5. **Der AStV wird daher gebeten, den Rat zu ersuchen, er möge den Entwurf von Schlussfolgerungen des Rates zu einer Strategie für das Informationsmanagement im Bereich der inneren Sicherheit in der EU in der in Anlage enthaltenen Fassung billigen.**
6. Auf Antrag der deutschen Delegation wird die nachstehende Erklärung in das Protokoll über die Ratstagung aufgenommen, auf der die Schlussfolgerungen gebilligt werden:

Deutschland unterstützt und billigt uneingeschränkt die im Haager Programm (Dok. 16054/04, Abschnitt III Nummer 2.1) und im Haager Aktionsplan (Dok. 9778/2/05 REV 2, Nummer 3.1 Buchstabe k) niedergelegte Idee, eine Strategie für das Informationsmanagement der EU festzulegen und umzusetzen. Deutschland unterstützt und billigt die heute verabschiedeten Schlussfolgerungen des Rates zu einer Strategie für das Informationsmanagement insoweit, als der grenzüberschreitende Informationsaustausch zwischen mit Strafsachen befassten Strafverfolgungs- und Justizbehörden innerhalb des bestehenden Rechtsrahmens der EU betroffen ist.

DER RAT DER EUROPÄISCHEN UNION –

UNTER HINWEIS AUF

- das Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union², insbesondere auf Nummer 2.1, in der ein verbesserter Informationsaustausch zur Kriminalitätsbekämpfung gefordert und deshalb der Verfügbarkeitsgrundsatz eingeführt wird;
- den Aktionsplan des Rates und der Kommission zur Umsetzung des Haager Programms zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union³, insbesondere auf Nummer 3.1 Buchstabe k, in dem die Festlegung einer Strategie für einen kohärenten Ansatz bei der Entwicklung von Informationstechnologien (IT) zur Unterstützung der Sammlung, der Speicherung, der Verarbeitung, der Analyse und des Austauschs von Informationen gefordert wird;
- den Bericht der Zukunftsgruppe der Innenminister, in dem die Umsetzung einer "Strategie der Europäischen Union des Informationsmanagements" (EU IMS) empfohlen wird, die darauf abzielt, dem Umstand abzuwehren, dass derzeit eine "unkoordinierte (...) und uneinheitliche (...) Palette an Informationssystemen und -instrumenten" existiert, die "Kosten und Verzögerungen, die sich nachteilig auf die operative Arbeit auswirken", verursacht haben, und so "den eingeschränkten Blickwinkel des Einzelfallansatzes aufzugeben und ein ganzheitliches Ziel für die Verwaltung strafverfolungsrelevanter Informationen ins Auge zu fassen";
- die Schlussfolgerungen des Rates zum Konvergenzprinzip und zur Struktur der inneren Sicherheit⁴ und die Maßnahmen im Anschluss an die informelle JI-Ministertagung im Bereich moderne Technologien und Sicherheit⁵;

² Dok. 16504/04 JAI 559.

³ Dok. 9778/2/05 REV 2 JAI 207.

⁴ Dok. 14069/08 JAI 514 CATS 78.

⁵ Dok. 10143/09 JAI 324 CATS 55 ASIM 54 ENFOPOL 145 CRIMORG 85.

- die Mitteilung der Europäischen Kommission vom 10. Juni 2009 mit dem Titel "Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger" (KOM(2009) 262), in der erklärt wird, dass es für die Sicherheit der EU leistungsfähiger Systeme für den Informationsaustausch zwischen den nationalen Behörden und den europäischen Stellen bedarf;
- den Umstand, dass der Europäische Rat im Stockholmer Programm das Erfordernis der Kohärenz und der Konsolidierung bei der Entwicklung von Informationsmanagement und -austausch anerkannt und den Rat ersucht hat, eine EU-Strategie für Informationsmanagement anzunehmen und umzusetzen, die Folgendes umfassen sollte: Entwicklung gemäß den Anforderungen der Praxis, eine solide Datenschutzregelung, die Interoperabilität von IT-Systemen und die Rationalisierung der verschiedenen Instrumente sowie umfassende Koordination, Konvergenz und Kohärenz;

AUFBAUEND AUF

- den Beratungen der Gruppe der Freunde des Vorsitzes⁶ über die technischen Modalitäten für die Umsetzung des Verfügbarkeitsgrundsatzes;
- den vorgeschlagenen Schlussfolgerungen des Rates⁷ zur Festlegung einer Strategie für einen kohärenten Ansatz bei der Entwicklung von Informationstechnologien (IT);
- den Schlussfolgerungen der COPE-Konferenzen von 2007, 2008 und 2009⁸ und dem Konzept der gemeinsamen Anforderungen (Common Requirements Vision)⁹;

⁶ Dok. 13558/1/05 REV 1.

⁷ Dok. 15478/05 CRIMORG 152 CATS 87.

⁸ Dok. 10063/07 CATS 70, 13592/08 CATS 74 und 14033/09 CATS 99.

⁹ Dok. 7758/08 CATS 21.

IN ANERKENNUNG DES FOLGENDEN:

Ein effizienter und sicherer grenzüberschreitender Informationsaustausch¹⁰ ist die Grundvoraussetzung für die Verwirklichung der Ziele für den Bereich der inneren Sicherheit in der Europäischen Union.

Voraussetzung hierfür ist, dass die richtige Information zum richtigen Zeitpunkt für die richtige Person am richtigen Ort verfügbar ist. Die Aufgaben der inneren Sicherheit sind auf eine ganze Reihe von Behörden aufgeteilt (die "Praxis"), und diese Aufteilung variiert von Mitgliedstaat zu Mitgliedstaat je nach den nationalen Strukturen, Zuständigkeiten und rechtlichen Rahmenbedingungen. In der Vergangenheit wurden Entscheidungen über den Informationsaustausch allzu oft von Gründen im Zusammenhang mit den jeweils beteiligten Organisationen abhängig gemacht, wodurch die betreffenden strukturellen Unterschiede zwischen den Mitgliedstaaten nicht berücksichtigt wurden und unnötig komplizierte Anforderungen an den Informationsaustausch entstanden.

Mit dem Haager Programm wurde im Hinblick auf den zukünftigen Informationsaustausch in der EU der Grundsatz der Verfügbarkeit eingeführt und festgelegt, dass im Hinblick darauf, "was die Methoden für den Informationsaustausch anbelangt", "die neuen Technologien in vollem Umfang genutzt werden" und "die Methoden (...) an jede Art von Informationen angepasst sein" sollten. Daher sollten zur Förderung des Austauschs zwischen den Mitgliedstaaten und zur Vereinfachung der praktischen Modalitäten für diesen Austausch die einschlägigen Informationen in einem geeigneten Format verfügbar sein; dies setzt voraus, dass bei den einzelstaatlichen Entscheidungen die Belange der Politikbereiche der EU berücksichtigt werden. Darüber hinaus müssen die betreffenden Mitgliedstaaten und Behörden ein hohes Maß an Vertrauen in das Informationsmanagement der jeweils anderen Mitgliedstaaten und Behörden haben können.

Ferner müssen in Bezug auf den Grundsatz der Verfügbarkeit die Erwartungen der Bürger im Hinblick auf den Schutz ihrer Privatsphäre und ihre Erwartungen hinsichtlich ihrer Sicherheit in ausgewogener Weise berücksichtigt werden.

In Anbetracht der Bandbreite der bestehenden Instrumente für den grenzübergreifenden Informationsaustausch haben die Mitgliedstaaten verschiedentlich zum Ausdruck gebracht, dass es notwendig ist, für Kohärenz und Konsolidierung zu sorgen, und dass erst die bestehenden Instrumente und Vereinbarungen umgesetzt werden müssen, bevor neue Initiativen ergriffen werden. Dies zeigt, dass es notwendig ist, das Informationsmanagement professioneller zu gestalten und zu straffen, und zwar auch in Bezug auf die Erhebung, die Speicherung, die Verarbeitung, die Analyse und den Austausch von Informationen.

¹⁰ In diesem Zusammenhang bezeichnet der Begriff "Information" alle Informationen oder strafrechtlichen Erkenntnisse, die die zuständigen Behörden der Mitgliedstaaten benötigen und die ihnen nach dem einschlägigen Rechtsrahmen zur Verfügung stehen, um das Ziel einer Verbesserung der inneren Sicherheit in der EU im Interesse der Unionsbürger zu erreichen.

Das Erfordernis der Kohärenz und Professionalisierung wird durch die zunehmende Mobilität der Bürger, die immer vielschichtiger werdende Kriminalität und die infolgedessen auch immer vielschichtiger werdenden Kriminalitätsbekämpfungsstrategien der EU sowie dadurch immer dringlicher, dass die EU und die Mitgliedstaaten ihre Ressourcen mit höchstmöglicher Wirkung einsetzen müssen.

Mit der Strategie für das Informationsmanagement soll die Verwaltung der von den zuständigen Behörden benötigten Informationen unterstützt, gestrafft und erleichtert werden, um die innere Sicherheit in der EU zu gewährleisten, wobei jedoch die Zuständigkeiten der Mitgliedstaaten für die Gewährleistung der inneren Sicherheit im Inland nicht berührt werden. Bei den betreffenden Behörden wird es sich im wesentlichen um die mit Strafsachen befassten Strafverfolgungs-, Grenzschutz- und Justizbehörden handeln. Der Notwendigkeit des Austauschs von Informationen mit anderen Behörden und Quellen wird jedoch ebenfalls Rechnung getragen werden.

Es ist eindeutig notwendig, zwischen den methodischen Werkzeugen für ein effizientes Informationsmanagement und den Zielen und Gründen für die Verarbeitung der Informationen zu unterscheiden. Letzteres (die "Prioritäten und Anforderungen für die Praxis") ergibt sich aus den vom Rat – insbesondere im Stockholmer Programm – vorgegebenen Prioritäten;

BESCHLIESST FOLGENDES:

1. Es wird eine Strategie für das Informationsmanagement mit dem Ziel festgelegt und durchgeführt, die Verwaltung der von den zuständigen Behörden benötigten Informationen zu unterstützen, zu straffen und zu erleichtern, um die innere Sicherheit in der EU zu gewährleisten; diese Strategie
 - a) beruht auf folgenden Grundsätzen:
 - Das Informationsmanagement stellt ein wesentliches Instrument für die Verwirklichung des Ziels einer Verbesserung der inneren Sicherheit in der EU und des Schutzes der Unionsbürger dar, bleibt aber ein Mittel zum Zweck und ist nicht Selbstzweck. Die für Informationsmanagement und -austausch vorgegebenen Prioritäten müssen den politischen, strategischen und operativen Prioritäten entsprechen und die Prioritäten der Praxis in Bezug darauf, wie die vorgenannten Ziele verwirklicht werden sollen, unterstützen.

- Das Informationsmanagement ist funktionsorientiert, d.h. es hängt im Gegensatz zu einem zuständigkeits- oder organisationsorientierten System von den zu bewältigenden Aufgaben ab. Daraus folgt, dass die EU-Strategie für das Informationsmanagement den disziplinübergreifenden Ansatz bereitstellt, der zum Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts benötigt wird; insbesondere bietet sie die Möglichkeit zu einem verstärkten Informationsaustausch und einer engeren Zusammenarbeit zwischen allen Beteiligten, damit die Bekämpfung der grenzüberschreitenden Kriminalität noch effizienter gestaltet werden kann.
 - Mit der Strategie wird eine Richtschnur für einen ausgewogenen Informationsaustausch vermittelt, bei dem die Weitergabe von Informationen sowohl dem Bedarf der Praxis als auch den Rechten des Einzelnen Rechnung trägt. Es werden die Voraussetzungen für eine fachgerechte, praxisorientierte, effiziente und kostenwirksame Entwicklung und Verwaltung des Informationsaustauschs festgelegt. Die Strategie zeigt den Weg hin zu einem strukturierten Informationsaustausch auf und bildet die Grundlage für eine verbesserte Entscheidungsfindung und Steuerung.
 - Die Strategie selbst bewirkt keine Vernetzung der unterschiedlichen Datenbanken und sieht auch keine speziellen Arten des Datenaustauschs vor, aber sie stellt sicher, dass – bei Vorliegen der operativen Anforderungen und einer Rechtsgrundlage – die einfachste, am leichtesten nachvollziehbare und kostenwirksamste Lösung gefunden wird;
- b) besteht aus acht Schwerpunktbereichen, die in die nachstehenden Rubriken untergliedert sind und im Anhang näher erläutert werden:
- I. Bedarf und Anforderungen
 1. Bedarf, Anforderungen und Mehrwert werden als Voraussetzung für die Entwicklung bewertet
 2. Die Entwicklung folgt vereinbarten Arbeitsabläufen im Bereich der Strafverfolgung und Modellen zur Gewinnung strafrechtlicher Erkenntnisse
 3. Die Entwicklung stützt sowohl die datenschutzrechtlichen Anforderungen als auch den praktischen operativen Bedarf
 - II. Interoperabilität und Kosteneffizienz
 4. Interoperabilität und Koordinierung werden sowohl in Bezug auf praktische Arbeitsabläufe als auch für technische Lösungen gewährleistet
 5. Wiederverwendung ist die Regel: das Rad ist nicht neu zu erfinden
 - III. Entscheidungs- und Entwicklungsprozesse
 6. Die Mitgliedstaaten werden von Anfang an in den Prozess eingebunden
 7. Für jeden Teil des Prozesses gibt es eine eindeutige Zuständigkeit, wodurch Kompetenz, Qualität und Effizienz sichergestellt werden

IV. Multidisziplinärer Ansatz

8. Die interdisziplinäre Koordinierung im JI-Bereich wird sichergestellt

2. es werden die nötigen Schritte eingeleitet, um einen detaillierten Aktionsplan zur Erfüllung der allgemeinen Zielsetzungen und Vorgaben dieser Strategie auszuarbeiten und erforderlichenfalls zu aktualisieren;

ERSUCHT

- die Vorbereitungsgremien des Rates, die sich mit Fragen des Informationsaustauschs und der Entwicklung von IT-Systemen befassen, die Strategie umzusetzen;
- den AStV, die Ad-hoc-Gruppe "Informationsaustausch" mit der Aufstellung einer Maßnahmenliste für die Umsetzung der Strategie zu betrauen und anhand der Berichterstattung durch diese und andere Gruppen für die kohärente und effiziente Umsetzung der Strategie zu sorgen;
- EU-Beamte und Vertreter der Mitgliedstaaten sowie Experten in den Gremien und Einrichtungen der EU, bei der Ausarbeitung von Entscheidungen, die unter anderem den Informationsaustausch auf bilateraler und regionaler Ebene und mit Drittstaaten oder Organisationen betreffen, der Strategie Rechnung zu tragen und diese bei der Entwicklung und Durchführung von Programmen und Projekten für den Informationsaustausch und die Entwicklung von IT-Systemen zu berücksichtigen;
- die Mitgliedstaaten, die auf EU-Ebene unternommenen gemeinsamen Bemühungen dadurch zu unterstützen, dass die Strategie auf nationaler Ebene als Leitlinie für politische Entscheidungsträger, IT-Beauftragte und sonstige Entscheidungsträger in den zuständigen Behörden herangezogen wird, wenn es um Fragen des internationalen Informationsaustauschs und der Entwicklung von IT-Systemen (auch das "National Housekeeping" sowie um die Beziehungen zu Drittstaaten oder Organisationen) geht oder diese eine Rolle spielen;
- die Kommission, die in diesen Schlussfolgerungen vereinbarten Methoden bei der Erstellung einer Mitteilung anzuwenden, die dem Rat bei der Formulierung von Prioritäten der Praxis für den Informationsaustausch für Strafverfolgungszwecke und bei der Ausarbeitung des europäischen Modells für den Informationsaustausch behilflich sein soll.

I. BEDARF UND ANFORDERUNGEN

1. Bedarf, Anforderungen und Mehrwert werden als Voraussetzung für die Entwicklung bewertet

Dieser Schwerpunktbereich sieht vor, dass vor Einführung eines neuen Informationsaustauschs jeweils der damit verbundene Mehrwert zu bewerten ist. Ferner gelangt das Konzept der Verfügbarkeit der Information, das sich auf Zweck, Notwendigkeit und Verhältnismäßigkeit stützt, zur Anwendung.

Es wird eine obligatorische Bewertung des Praxisbedarfs sowie der praktischen und gesetzlichen Anforderungen für die betreffende Zusammenarbeit erfolgen, auch eine Bewertung der Frage, wie die Lösungen angewandt werden und wie nützlich sie sind, um die effektive operative Zusammenarbeit und die entsprechenden Arbeitsmethoden zu verbessern.

Daher wird sich die Entwicklung auf den Bedarf und die Anforderungen der einbezogenen Behörden stützen und an ihnen orientieren. Eine Bewertung der Nützlichkeit (einschließlich einer Kosten-Nutzen-Analyse) wird auch dazu beitragen, Prioritäten für die Entwicklung festzusetzen.

Das bedeutet:

- a) *Wenn Initiativen betreffend den Informationsaustausch oder technische Lösungen auf die Agenda gesetzt werden, sind Endnutzer und die Managementebene in verschiedenen Bereichen einzubeziehen, da ohne ihre Unterstützung Bedeutung und Wert einer Initiative nicht beurteilt werden können. Ihre Einbeziehung ist darüber hinaus wichtig, wenn es darum geht, für Ausgewogenheit zwischen Datenschutz und Praxisbedarf zu sorgen;*
- b) *Überlegungen oder Erörterungen zu technischen Lösungen sind an der Bedarfs- und Anforderungsanalyse auszurichten;*
- c) *Beratungen über Rechtssetzungsakte und/oder Vorstudien für technische Lösungen sollten nicht aufgenommen werden, bevor nicht die Praxisanforderungen ermittelt und dokumentiert wurden;*
- d) *jede Initiative im Bereich des Informationsaustauschs muss auf einer eingehenden Analyse der auf EU-Ebene und in den Mitgliedstaaten vorhandenen Lösungen, auf der Festlegung von Bedarf, Anforderungen und Mehrwert sowie auf der Bewertung der rechtlichen, technischen und finanziellen Auswirkungen der neuen Initiative beruhen;*
- e) *es sollten eindeutige Bewertungskriterien entwickelt werden, die an systematische Evaluierungsprogramme gekoppelt sind;*
- f) *die Bewertung der Frage, ob es zweckmäßig ist, beispielsweise bestimmte Informationsarten weiterzuentwickeln, sollte sich aus einem Prozess der Bestimmung strategischer Prioritäten ableiten.*

2. Die Entwicklung folgt vereinbarten Arbeitsabläufen und Modellen zur Gewinnung strafrechtlicher Erkenntnisse

Die Verbesserung des Informationsaustauschs hängt in sehr starkem Maße davon ab, inwieweit dieser durch IT-Lösungen unterstützt wird. Um den Informationsaustausch zu fördern, muss die Informationstechnologie die Arbeitsabläufe im Rahmen der grenzüberschreitenden Zusammenarbeit im Bereich der Strafverfolgung unterstützen.

Die Arbeitsabläufe müssen einen raschen, effizienten, nutzerfreundlichen und kostenwirksamen Austausch von Informationen und strafrechtlichen Erkenntnissen ermöglichen. Zu diesem Zweck müssen die einzelnen Arbeitsschritte genau beschrieben, bekannt und zugänglich sein. Sie sollten fester Bestandteil der Systementwicklung und -beschaffung sein. Dadurch werden Management und Dokumentation der Entwicklung verbessert, und die Entwicklung wird durch den Bedarf der grenzüberschreitenden Zusammenarbeit im Bereich der Strafverfolgung gesteuert.

Das bedeutet:

- a) *Die Arbeit an dem derzeitigen Konzept der gemeinsamen Anforderungen (Common Requirements Vision, CRV) sollte fortgesetzt und durch zusammen mit bzw. von den nationalen Behörden vorgenommene Analysen wesentlicher Anforderungen ergänzt werden;*
- b) *eine "Informations-Landkarte" (information map) sollte einen Überblick über die Arbeitsabläufe und die entsprechenden Informationsflüsse der grenzüberschreitenden Zusammenarbeit ermöglichen, damit auf dieser Grundlage die Schnittstellen ermittelt werden können, an denen eine Koordinierung erforderlich ist.*

3. Die Entwicklung stützt sowohl die datenschutzrechtlichen Anforderungen als auch den praktischen operativen Bedarf

Die Zusammenarbeit zur Gewährleistung der inneren Sicherheit in der EU stellt hohe Anforderungen an den Datenschutz einschließlich der Datensicherheit. So sind sowohl der Schutz der Privatsphäre als auch die Sicherheit der Arbeitsabläufe sicherzustellen, während für den Bedarf der Praxis die Nutzung und der Austausch von Informationen ermöglicht werden muss.

Ein hohes Maß an Sicherheit wird zugleich die Belange der Praxis und das Privatleben der Bürger schützen, ohne dass die Verfügbarkeit von Informationen beeinträchtigt wird, so dass den berechtigten Nutzern in nachprüfbarer Weise korrekte Informationen bei Bedarf zur Verfügung stehen, wenn dies nach den geltenden Rechtsvorschriften zulässig ist. Durch die angemessene Nutzung moderner Technologien, aber auch die Anpassung der Arbeitsabläufe und Maßnahmen zur Umsetzung des Datenschutzes wird dieses erleichtert. Ein verstärktes Vertrauen in diesen Bereichen zwischen den zuständigen Behörden ist ein wichtiger Schritt hin zu einer standardmäßigen gemeinsamen Nutzung von Daten.

Das bedeutet:

- a) *Die gesetzlichen Anforderungen an den Schutz personenbezogener Daten und an Sicherheitsstandards müssen zusammen mit dem Bedarf der Praxis an Nutzung und Austausch von Informationen bewertet werden, damit für den Informationsaustausch und für die IT-Systeme das korrekte Maß an praxisbezogenen und technischen Sicherheitsstandards gewährleistet wird;*
- b) *die Sammlung von Daten muss gezielt erfolgen, damit die Privatsphäre des Einzelnen geschützt, eine Informationsüberflutung der zuständigen Behörden verhindert und eine effiziente Kontrolle der Informationen erleichtert wird;*
- c) *die Datensicherheit muss durch organisatorische sowie technische und physische Maßnahmen gewährleistet werden;*
- d) *die verschiedenen Instrumente, wie etwa Anwendungen und Hilfsprogramme, müssen im Interesse einer Arbeitserleichterung für die zuständigen Behörden und die Endnutzer gestrafft werden; dadurch sowie durch eine Schulung betreffend die zur Verfügung stehenden Instrumente und deren Nutzung wird das Schadensrisiko möglichst gering gehalten werden;*
- e) *angemessene Maßnahmen zur Umsetzung des Datenschutzes müssen sachgemäße und regelmäßige operationelle Kontrollen vorsehen und sicherstellen, dass bei Verstößen angemessene Strafen auch wirklich zur Anwendung kommen;*
- f) *zur Bewertung der Qualität und der Auswirkungen von Datenschutz- und Datensicherheitsmaßnahmen sollten systematische Evaluierungs- und Überwachungsverfahren entwickelt werden.*

II. INTEROPERABILITÄT UND KOSTENEFFIZIENZ

4. Interoperabilität und Koordinierung werden sowohl in Bezug auf praktische Arbeitsabläufe als auch für technische Lösungen gewährleistet

Die Interoperabilität betrifft vielerlei Ebenen, wie etwa die gesetzliche, die inhaltliche, die praktische und die technische Ebene. Sie ist die Voraussetzung für einen effizienten Informationsaustausch und erleichtert diesen zugleich. Interoperable Lösungen und Kapazitäten gründen sich auf Initiativen und Vorschläge, die ihrerseits vom Bedarf und von den Anforderungen der Praxis ausgehen.

Technisch sollten IT-Lösungen und ihre Komponenten gemeinsam vereinbarten Standards und Grundsätzen entsprechen. Es sollten Standardlösungen angewandt und auf ein Mindestmaß beschränkt werden.

Ihre Anwendung wird für eine größere Kohärenz bei der Entwicklung und Verwaltung von Lösungen sorgen.

Sie wird auch die Interoperabilität und Koordinierung zwischen Systemen fördern. Daher werden bestehende Lösungen besser und stärker genutzt werden; so können die IT-Systeme größere Teile der Arbeitsabläufe unterstützen. Die Notwendigkeit einer doppelten Speicherung und doppelten Registrierung wird abnehmen und die IT-Unterstützung wird benutzerfreundlicher werden. Durch die Anwendung von gemeinsam vereinbarten Standards kann der Informationsaustausch von mehreren Zulieferern statt nur von einem Zulieferer unterstützt werden, so dass die Abhängigkeit von speziellen Zulieferern auf ein Mindestmaß reduziert wird. Langfristig werden dadurch auch die Anpassungskosten in den Mitgliedstaaten gesenkt.

Das bedeutet:

- a) *Die "Informations-Landkarte" sollte einen vergleichenden Überblick über die Rechtslage auf Ebene der EU und der Mitgliedstaaten im Bereich des Informationsaustauschs enthalten;*
- b) *die in der europäischen Interoperabilitätsstrategie enthaltenen Empfehlungen sollten berücksichtigt werden;*
- c) *bestehende, gemeinsam vereinbarte Akkreditierungs-/Standardisierungsfunktionen sollten verwendet werden;*
- d) *Möglichkeiten zur Systemintegration, wie z.B. Standardtechnologien and -fähigkeiten, die die Systemintegration erleichtern und darauf abzielen, Sicherheit, Skalierbarkeit und Leistung zu gewährleisten, sollten ermittelt werden;*
- e) *Datenschutz- und Datensicherheitsmaßnahmen sollten sowohl auf EU- als auch auf nationaler Ebene sowie zwischen beiden Ebenen koordiniert werden.*

5. Wiederverwendung ist die Regel: das Rad ist nicht neu zu erfinden

Die Entwicklung ist mit hohen Kosten und erheblichen Investitionen verbunden, aber auch mit langfristigen Kosten für Verwaltung, Wartung und Support. Normalerweise fließt lediglich ein kleiner Teil der Gesamtkosten in die Entwicklungsphase. Dies ist nicht nur für die technische Entwicklung von Bedeutung, sondern auch im Hinblick darauf, dass keine neuen Rechtsgrundlagen oder praktischen Modalitäten festgelegt werden, wenn bestehende Rechtsgrundlagen oder Modalitäten genutzt bzw. erweitert werden können.

Daher muss die gemeinsame Nutzung und Wiederverwendung von nachhaltigen Lösungen eine Priorität in Bezug auf die Entwicklung und technische Verbesserungen darstellen. Die Wiederverwendung trägt dazu bei, dass Parallellösungen vermieden und bestehende Instrumente und Systeme, auch hinsichtlich ihrer Integration und Zweckmäßigkeit, weiterentwickelt werden. Infolgedessen werden frühere Investitionen verstärkt genutzt werden und wird ein geringerer Bedarf an neuen Investitionen bestehen. Je mehr Komponenten zur Verfügung stehen, desto weniger Zeit wird für die Entwicklung erforderlich sein.

Für eine effiziente Wiederverwendung ist eine "Informations-Landkarte", die einen Überblick über die bestehenden Informationsströme, -funktionen und -komponenten bietet, Voraussetzung. Die effiziente (Wieder-)Verwendung von erfolgreichen Lösungen erfordert außerdem einen konstanten Evaluierungsprozess und ein Beobachtungsinstrument, damit festgestellt werden kann, wie der Informationsaustausch funktioniert.

Das bedeutet:

- a) *Die "Informations-Landkarte" sollte Informationsströme, -funktionen und -lösungen einbeziehen;*
- b) *ein pragmatischer, sachbezogener und ressourceneffizienter Evaluierungsmechanismus muss geschaffen werden. Er sollte zweck- und nicht zuständigkeitsorientiert sein; er sollte nicht auf bestimmte (Rechts-)Instrumente beschränkt sein, und es sollte sichergestellt werden, dass Erfahrungswerte aus früheren Evaluierungen genutzt werden können;*
- c) *zur Beurteilung der Wirkung ihrer Tätigkeit muss die EU Instrumente schaffen, um nicht nur die kriminellen Aktivitäten messen zu können, sondern auch die Wirksamkeit ihrer Anstrengungen zur Gewährleistung der inneren Sicherheit in der EU, vor allem hinsichtlich der Entwicklung des Informationsaustauschs;*
- d) *unter Berücksichtigung von Verfahren, die nicht nur aus der EU, sondern auch aus Drittländern stammen, sollte ein Modell für die gemeinsame Nutzung und Wiedernutzung nachhaltiger Lösungen ausgearbeitet werden;*
- e) *Instrumente, die derzeit für den Informationsaustausch genutzt werden, sollten eingehend auf ihre Effizienz und Wirksamkeit hin überprüft werden, damit sie gestrafft werden können (auf jeden Fall, bevor damit begonnen wird, neue Instrumente zu entwickeln).*

III. ENTSCHEIDUNGS- UND ENTWICKLUNGSPROZESSE

6. Die Mitgliedstaaten werden von Anfang an in den Prozess eingebunden

Entscheidungen auf EU-Ebene über Zusammenarbeit, Informationsaustausch und Entwicklung von IT-Systemen haben erhebliche Auswirkungen – und zwar sowohl kurzfristig als auch aus einer "Lebenszyklus"-Perspektive – auf die Arbeitsabläufe, Strukturen, Investitionen und Haushalte der Mitgliedstaaten. Ein voll funktionsfähiges Endergebnis erfordert intensive Koordinierung auf nationaler Ebene sowie Gegenseitigkeit und Zusammenwirken zwischen der nationalen und der EU-Ebene.

Die Behörden der Mitgliedstaaten, die für die nationale Umsetzung von Arbeitsabläufen, Methoden und Entwicklungen zuständig sind, müssen bereits vom Beginn der Entwicklungsprozesse auf europäischer Ebene an eingebunden werden. Um einen umfassenden Beitrag leisten zu können, sollten die Mitgliedstaaten, sowohl was die Arbeitsabläufe als auch was die Technik betrifft, im eigenen Bereich für Interoperabilität sorgen und ihre eigenen Entwicklungsprozesse festlegen.

Das bedeutet:

- a) *die Informationsmanagementstrategien oder -maßnahmen auf nationaler und auf EU-Ebene sollten miteinander im Einklang stehen;*
- b) *Endnutzer und maßgebliche Interessenvertreter sollten sowohl auf nationaler als auch auf EU-Ebene einbezogen werden;*
- c) *die Behörden in den Mitgliedstaaten müssen ihre eigenen Entwicklungsprozesse ermitteln und gestalten.*

7. Für jeden Teil des Prozesses gibt es eine eindeutige Zuständigkeit, wodurch Kompetenz, Qualität und Effizienz sichergestellt werden

Um den Entwicklungsprozess besser steuern zu können, müssen die Rollen und Zuständigkeiten der einzelnen Akteure eindeutig festgelegt werden. In verschiedenen Bereichen, wie z.B. Aufgabenstruktur und Systemarchitektur (*business and technical architecture*), Methoden und Modelle, Management, Finanzen und Kontrolle, sind besondere Zuständigkeiten erforderlich. Beratungen über (technische) Lösungen müssen auf Ebene der geeigneten systemtechnischen und -architektonischen Zuständigkeiten erfolgen. Entscheidungen auf der Managementebene oder der politischen Ebene müssen auf die für diese Ebene geeigneten Themen abstellen.

So werden die Rollen ermittelt, die Zuständigkeiten festgelegt und die Strukturen geschaffen werden müssen, um sicherzustellen, dass alle betroffenen Parteien auf der richtigen Ebene und in der richtigen Phase des Prozesses eingebunden werden, aber auch um sicherzustellen, dass insgesamt für Koordinierung und Kohärenz gesorgt ist.

Das bedeutet:

- a) *die Rollen und Zuständigkeiten auf den verschiedenen Ebenen (innerhalb der nationalen Behörden, der Organe, Einrichtungen, Ämter und Agenturen der EU usw.) müssen ermittelt und organisiert werden;*
- b) *die Funktionen zur Vorbereitung der strategischen Entscheidungen betreffend Informationsmanagement und Entwicklung von IT-Systemen müssen ermittelt/festgelegt werden;*
- c) *Funktionen für Verwaltung, Weiterentwicklung und Evaluierung von (praxisbezogenen und technischen) Lösungen müssen vorhanden sein.*

IV. MULTIDISZIPLINÄRER ANSATZ¹¹

8. Die multidisziplinäre Koordinierung wird sichergestellt

Die Strategie für Informationsmanagement anerkennt und berücksichtigt den multidisziplinären Ansatz, der notwendig ist, um für innere Sicherheit zu sorgen und – unabhängig von der im Besitz der Informationen befindlichen Stelle – die Weitergabe und Wiederverwendung von Informationen zu erleichtern. Die moderne Technologie gestattet es, das gewünschte Verfügbarkeitsniveau zu erreichen, das es seinerseits ermöglicht, Störungen und die manuelle Wiedereingabe auf ein Mindestmaß zu beschränken und die Qualität der Informationen zu verbessern. Dieselbe Technologie ermöglicht es, das Datenschutzniveau, einschließlich des Datensicherheitsniveaus, beizubehalten oder zu erhöhen.

Die Strategie zielt darauf ab, den Informationsaustausch zwischen den zuständigen Behörden in funktioneller und technischer Hinsicht zu erleichtern, wenn dieser gesetzlich vorgesehen ist. Daher erfordert die Strategie Mittel zur Gewährleistung der Interoperabilität und sieht derartige Mittel vor. Dies bedeutet, dass die Anstrengungen zur Verwirklichung der Interoperabilität ein Zusammenwirken zwischen allen zuständigen Behörden und Organisationen erfordern. Welche Behörden und Organisationen dies sind, wird sich nach dem jeweils zu deckenden Bedarf richten. Mit der in dieser Strategie dargelegten Methodik – insbesondere den Schwerpunktbereichen 1 bis 3 – wird dafür gesorgt, dass die Interoperabilität zwischen den unmittelbar für die innere Sicherheit der EU zuständigen Behörden und über diese Behörden hinaus gewährleistet wird, wann immer dies erforderlich und verhältnismäßig ist, wobei allerdings auch dafür gesorgt wird, dass die Interoperabilität auf diese Fälle beschränkt ist.

¹¹ **DE: Prüfungsvorbehalt.**

Das bedeutet:

- a) *Der Informationsaustausch darf nicht durch Fragen der Zuständigkeit behindert werden (gegenseitige Anerkennung von verschiedenen nationalen Strukturen), wobei gleichzeitig der geltende Rechtsrahmen für diesen Austausch uneingeschränkt einzuhalten ist;*
- b) *IT-Unterstützung und -Standardisierung (einschließlich Architekturgrundsätze und Informations-/Datenmodelle) müssen so horizontal wie möglich angelegt sein und sich auf gemeinsame Grundsätze und Koordinierung stützen;*
- c) *Datenschutz- und Datensicherheitsmaßnahmen sollten zwischen der EU-Ebene und den Mitgliedstaaten koordiniert werden.*
