RAT DER EUROPÄISCHEN UNION

Brüssel, den 27. Januar 2012 (30.01)
(OR. en)

5833/12
ADD 2

Interinstitutionelles Dossier: 2012/0010 (COD)

DATAPROTECT 6
JAI 41
DAPIX 9
FREMP 8
COMIX 59
CODEC 217

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	27. Januar 2012
Empfänger:	der Generalsekretär des Rates der Europäischen Union, Herr Uwe CORSEPIUS
Nr. Komm.dok.:	SEK(2012) 73 endgültig
Betr.:	Arbeitsdokument der Kommissionsdienststellen Zusammenfassung der Folgenabschätzung Begleitunterlage zu der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) und der Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhüttung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

Die Delegationen erhalten in der Anlage das Kommissionsdokument SEK(2012) 73 endgültig.

Anl.: SEK(2012) 73 endgültig

EUROPÄISCHE KOMMISSION

Brüssel, den 25.1.2012
SEK(2012) 73 endgültig

ARBEITSDOKUMENT DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zu der

Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) und der Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

{KOM(2012) 10 endgültig}
{KOM(2012) 11 endgültig}
{SEK(2012) 72 endgültig}

ARBEITSDOKUMENT DER KOMMISSIONSDIENSTSTELLEN

ZUSAMMENFASSUNG DER FOLGENABSCHÄTZUNG

Begleitunterlage zu der

Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) und der Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr

1. EINFÜHRUNG

Seit 1995, als die derzeit geltenden Datenschutzvorschriften der EU verabschiedet wurden, sind infolge der raschen Veränderungen in Technologie und Wirtschaft neue Herausforderungen für den Datenschutz entstanden. Datenaustausch und Datenerfassung haben sich exponentiell entwickelt. Die Technik macht es möglich, dass Privatwirtschaft und Staat in einem noch nie dagewesenen Umfang auf personenbezogene Daten zugreifen. Gleichzeitig stellen immer mehr Personen ihre persönlichen Daten weltweit öffentlich zur Verfügung, ohne sich alle Risiken bewusst zu machen.

Um die wirtschaftliche Entwicklung zu sichern, muss Vertrauen in die Online-Umgebung geschaffen werden. Mangelt es Verbrauchern an Vertrauen, meiden diese Online-Einkäufe und -Dienste, darunter auch elektronische Verwaltungsdienste. Wenn nichts geschieht, wird das mangelnde Vertrauen die Entwicklung innovativer Anwendungen neuer Technologien weiter hemmen, das Wirtschaftswachstum behindern und eine sinnvolle Digitalisierung der behördlichen Dienste verhindern.

Darüber hinaus wurde mit dem Vertrag von Lissabon in Artikel 16 AEUV eine neue Rechtsgrundlage für ein moderneres und umfassendes Konzept für den Datenschutz und den freien Verkehr personenbezogener Daten geschaffen, das auch den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen abdeckt.

2. PROBLEMSTELLUNG

Die Folgenabschätzung befasst sich mit drei Hauptproblemen:

2.1. Problem 1: Hindernisse für Wirtschaft und Behörden durch Unterschiede in den Rechtsregelungen, Rechtsunsicherheit und uneinheitliche Durchsetzung

Ungeachtet der Zielsetzung der Richtlinie, in der EU ein gleichmäßiges Datenschutzniveau zu gewährleisten, sind die Vorschriften der Mitgliedstaaten nach wie vor sehr uneinheitlich. Daher kommt es vor, dass die für die Verarbeitung Verantwortlichen in der EU mit 27 unterschiedlichen Regelungen und Anforderungen konfrontiert sind. Die dadurch bedingte

Zersplitterung des Rechtsrahmens hat zu Rechtsunsicherheit und ungleichem Datenschutz geführt. Für die Wirtschaft ist dies mit unnötigen Kosten und einem **Verwaltungsaufwand** (mit Kosten in Höhe von **rund 3 Mrd. EUR pro Jahr** im Basisszenario) verbunden, und es könnte Unternehmen; darunter KMU, im Binnenmarkt von einer Expansion über Grenzen hinweg abhalten.

Darüber hinaus bestehen erhebliche Unterschiede zwischen den Mitgliedstaaten, was die Ressourcen und Befugnisse der für den Datenschutz zuständigen nationalen Behörden anbelangt. In manchen Fällen sind sie nicht in der Lage, ihren Durchsetzungsauftrag zufriedenstellend auszuführen. Auch gewährleistet die Zusammenarbeit zwischen den Behörden auf europäischer Ebene – über die bestehende Beratergruppe (Artikel-29-Datenschutzgruppe) – nicht immer, dass die Bestimmungen einheitlich angewandt werden. Sie muss daher verbessert werden.

2.2. Problem 2: Schwierigkeiten bei der Kontrolle der eigenen personenbezogenen Daten

Wegen der unzulänglichen Harmonisierung der einzelstaatlichen Datenschutzvorschriften und der unterschiedlichen Befugnisse der nationalen Datenschutzbehörden hat es der Einzelne in manchen Mitgliedstaaten schwerer als in anderen, seine Datenschutzrechte - besonders im Internet - wahrzunehmen.

Hinzu kommt, dass der Einzelne keine richtige Kontrolle mehr über seine eigenen Daten hat, da täglich immens viele Daten ausgetauscht werden und er oft nicht einmal weiß, dass seine personenbezogenen Daten erfasst werden. Zwar sind viele Europäer der Meinung, dass eine zunehmende Weitergabe personenbezogener Daten im modernen Leben normal ist[1], doch haben 72 % der Internetbenutzer in Europa immer noch Vorbehalte, wenn sie nach zu vielen personenbezogenen Daten gefragt werden. Sie wissen oft nicht, wie sie im Internet ihre Rechte wahrnehmen können.

2.3. Problem 3: Datenschutzlücken und Unstimmigkeiten beim Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Die polizeiliche und justizielle Zusammenarbeit in Strafsachen war ausdrücklich vom Geltungsbereich der Richtlinie ausgenommen, deren Rechtsgrundlage auf den Binnenmarkt ausgelegt ist. Was den Rahmenbeschluss von 2008 über den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen anbelangt, so spiegelt dieser die frühere Säulenstruktur der EU wider. Sein **Geltungsbereich** ist **beschränkt** und er enthält verschiedene andere **Lücken,** die bei Einzelpersonen und Strafverfolgungsbehörden zu Rechtsunsicherheit und daneben zu praktischen Umsetzungsproblemen führen. Darüber hinaus lässt der Rahmenbeschluss einen erheblichen Spielraum für Ausnahmen von den Datenschutzgrundsätzen auf nationaler Ebene, so dass eine Harmonisierung ausbleibt. Dadurch könnten nicht nur diese Grundsätze ausgehöhlt werden – mit negativen Folgen für das Grundrecht des Einzelnen auf den Schutz seiner personenbezogenen Daten in diesem Bereich –, sondern könnte auch der Austausch personenbezogener Daten zwischen den zuständigen nationalen Behörden behindert werden.

---

[1] Siehe Eurobarometer Spezial 359 – „*Attitudes on Data Protection and Electronic Identity in the European Union*“, Juni 2011, S. 23.

3. SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

Im Hinblick auf die beschriebene Problematik zeigt die Subsidiaritätsanalyse, dass aus folgenden Gründen Maßnahmen auf EU-Ebene notwendig sind:

- Das Recht auf Schutz personenbezogener Daten ist in Artikel 8 der Charta der Grundrechte verankert. Rechtsgrundlage für Datenschutzvorschriften der EU ist Artikel 16 AEUV;
- personenbezogene Daten können immer schneller über Grenzen hinweg (zu anderen EU-Staaten und zu Drittländern) weitergegeben werden. Daneben stellen sich praktische Herausforderungen bei der Durchsetzung der Datenschutzvorschriften. Auch ist eine Zusammenarbeit zwischen den Mitgliedstaaten und ihren Behörden erforderlich. In diesem Bereich besteht Handlungsbedarf auf EU-Ebene, damit Kohärenz und ein hohes Maß an Datenschutz in der Union gewährleistet werden können;
- die Mitgliedstaaten können der derzeitigen Probleme – besonders im Zusammenhang mit der Uneinheitlichkeit der einzelstaatlichen Bestimmungen zur Umsetzung der EU-Datenschutzvorschriften - nicht allein Herr werden.
- Auch wenn die Mitgliedstaaten Maßnahmen ergreifen können, um Datenschutzverstöße zu unterbinden, bestünde ohne gemeinsame EU-Vorschriften die Gefahr, dass der Datenschutz in den Mitgliedstaaten nicht in gleichem Maße gewährleistet ist, was den grenzüberschreitenden Verkehr personenbezogener Daten behindern würde.

Die **geplanten Maßnahmen entsprechen dem Verhältnismäßigkeitsgrundsatz:** Sie fallen in den Zuständigkeitsbereich der Union nach den Verträgen und sind notwendig, um die einheitliche Anwendung der EU-Vorschriften sowie einen wirksamen und gleichmäßigen Schutz der Grundrechte von Einzelpersonen sicherzustellen. Um weiterhin für einen glaubwürdigen, hohen Anforderungen genügenden Datenschutz in der globalisierten Welt zu sorgen, ohne den freien Datenverkehr zu beeinträchtigen, ist es notwendig, auf EU-Ebene Maßnahmen zu ergreifen. Wenn der Binnenmarkt reibungslos funktionieren soll, müssen die Vorschriften gleiche Wettbewerbsbedingungen für Unternehmen gewährleisten.

4. ZIELE

Die drei **Hauptziele** sind:

- **Vertiefung der Binnenmarktdimension des Datenschutzes** durch Abbau der Unterschiede in den Regelungen, Verbesserung der Kohärenz und **Vereinfachung** des Regelungsumfelds, damit unnötige Kosten vermieden werden und der **Verwaltungsaufwand** verringert wird;

- **Stärkung des Grundrechts auf Datenschutz und Übertragung der Kontrolle über die Daten an die Betroffenen**;

- **Stärkung der Kohärenz der EU-Datenschutzvorschriften** – auch im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen - unter voller Berücksichtigung des Inkrafttretens des Vertrags von Lissabon.

5. OPTIONEN

5.1. Option 1: Weiche Maßnahmen

Hierbei handelt es sich hauptsächlich um **Mitteilungen der Kommission zur Auslegung der Rechtsvorschriften, technische Hilfsmittel und finanzielle Unterstützung** – sowie um **Maßnahmen zur Förderung der Standardisierung und Selbstregulierung** –, wodurch die für die Datenverarbeitung Verantwortlichen dazu angehalten werden sollen, die geltenden Regeln in der Praxis anzuwenden, und die Bevölkerung sensibilisiert werden soll. Die Kommission würde **nur in sehr begrenztem Umfang Änderungen an den Rechtsvorschriften** vorschlagen, um Konzepte der Richtlinie klarzustellen und bestimmte Fragen anzugehen, die auf anderem Wege nicht wirksam gelöst werden können. Die Option käme nur für die Probleme 1 und 2 in Frage.

Bei einer begrenzten Änderung der Rechtsvorschriften würden der Transparenzgrundsatz und das Prinzip der Datensparsamkeit ausdrücklich festgeschrieben und eine Rechtsgrundlage für verbindliche unternehmensinterne Vorschriften für internationale Datentransfers eingeführt werden.

5.2. Option 2: Aktualisierung der Regelung

Die Kommission würde **Rechtsvorschriften zur weiteren Harmonisierung der materiellrechtlichen Vorschriften vorschlagen**, um bestimmte Vorschriften klarer zu formulieren und Inkohärenzen aufgrund unterschiedlicher Ansätze in den Mitgliedstaaten zu beseitigen. Diese Vorschläge könnten eine Lösung für die Probleme 1 und 2 bieten, da einerseits der **Datenverkehr innerhalb der EU und zwischen der EU und Drittländern erleichtert würde** und andererseits **die Rechte des Einzelnen (**darunter das Auskunftsrecht, das Recht auf Vergessenwerden, klarere Modalitäten für die Einwilligung und für die Meldung von Datenschutzverstößen) **klar dargelegt und gestärkt werden würden und den für die Datenverarbeitung Verantwortlichen und den Auftragsverarbeitern mehr Verantwortung – verbunden mit einer strengeren Rechenschaftspflicht – übertragen werden würde** (z. B. gegebenenfalls durch die Einführung der Pflicht zur Ernennung von Datenschutzbeauftragten oder zur Durchführung von Datenschutz-Folgenabschätzungen**)**. Diese Option würde insbesondere eine „**zentrale Anlaufstelle**“ für die für die Verarbeitung Verantwortlichen vorsehen (d. h. eine einzige zuständige Datenschutzbehörde im Rahmen einer einheitlichen Rechtsregelung). Die allgemeinen Meldeanforderungen würden vereinfacht („einfache Dokumentierung“). Auch würden die **Datenschutzbehörden unabhängiger** gemacht und ihre **Befugnisse harmonisiert werden.** Vorgesehen wären außerdem eine engere Zusammenarbeit und gegenseitige Unterstützung der Datenschutzbehörden unter anderem durch ein neues **Kohärenzverfahren**, in das sowohl ein neu zu schaffendes europäisches Datenschutzgremium als auch die Kommission eingebunden werden sollen.

Für den Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (Problem 3) würde die Kommission Vorschläge zur Ersetzung des Rahmenbeschlusses durch ein **neues Instrument mit erweitertem Geltungsbereich** vorlegen und die **wichtigsten Lücken und Mängel** angehen, um unter Berücksichtigung der Besonderheiten des Strafverfolgungsbereichs sowohl die Rechte des Einzelnen zu stärken als auch die Zusammenarbeit zwischen den Strafverfolgungsbehörden zu fördern.

5.3. Option 3: Detaillierte Rechtsregelung auf EU-Ebene

Diese Option würde sämtliche Elemente der Option 2 sowie eine **sehr viel detailliertere EU-Rechtsregelung** beinhalten, darunter sektorspezifische Vorschriften (z. B. für das Gesundheitswesen) sowie eine **zentralisierte Durchsetzungsstruktur auf EU-Ebene (**d. h. Einrichtung einer Datenschutzbehörde der EU). Sie würde auch die Abschaffung der allgemeinen Meldeanforderungen (mit Ausnahme der Vorabkontrolle bei einer risikobehafteten Datenverarbeitung), die Einrichtung einer EU-weiten Zertifizierungsregelung für Verfahren und Produkte, die die Datenschutzanforderungen erfüllen, sowie die Definition EU-weit harmonisierter strafrechtlicher Sanktionen für Datenschutzverstöße vorsehen. Die Einwilligung würde als hauptsächliche Grundlage für eine Datenverarbeitung gelten.

Bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen würde diese Option neben den materiellrechtlichen Maßnahmen der Option 2 die Einführung ausführlicher Regeln für das (stets direkte) Auskunftsrecht von Einzelpersonen umfassen. Zudem würden die **einschlägigen Bestimmungen in allen geltenden Rechtsvorschriften der früheren dritten Säule** geändert und ganz an die neuen, ausgeweiteten harmonisierten Regeln angepasst werden.

6. FOLGENABSCHÄTZUNG

6.1. Option 1: Weiche Maßnahmen

Mitteilungen der Kommission zur Auslegung von Bestimmungen der Richtlinie wären nicht verbindlich und hätten somit **nur eine begrenzte Auswirkung, was die Rechtsunsicherheit und die Kosten anbelangt**. Eine umfassendere Selbstregulierung auf EU-Ebene könnte den für die Verarbeitung Verantwortlichen in bestimmten Sektoren mehr rechtliche Klarheit geben, sie **würde aber** eine wirksame, kohärente Anwendung der Bestimmungen mangels einer klaren, harmonisierten EU-Regelung an der Basis nicht **gewährleisten können**.

Sensibilisierungskampagnen würden dazu beitragen, Personen besser über ihre Datenschutzrechte und die Wahrnehmung dieser Rechte in der Praxis aufzuklären. Dadurch kann allerdings **nicht garantiert werden**, dass der Einzelne seine Rechte wahrnehmen kann, wenn diese Rechte in den Rechtsvorschriften nicht klar definiert sind. **Klarstellungen in den Rechtsvorschriften,** was die Grundsätze der Transparenz, der Datensparsamkeit und der Angemessenheit sowie verbindliche unternehmensinterne Datenschutzregelungen anbelangt, brächten Fortschritte in Bezug auf die Harmonisierung und die Rechtssicherheit für den Einzelnen und die Wirtschaft.

Hinsichtlich der Durchsetzung könnte die Kommission anhand von Mitteilungen die Vorbehalte der Mitgliedstaaten gegen eine dahingehende Änderung der innerstaatlichen Vorschriften nicht ausräumen, dass die Datenschutzbehörden unabhängiger gemacht und ihnen die gleichen Befugnisse wie in den anderen Ländern erteilt werden. Eine bessere Koordinierung mit der WP29 und ein Austausch zwischen den Datenschutzbehörden gäben positive Impulse für eine kohärentere Durchsetzung der Regeln. **Sollten die Vorschriften jedoch weiterhin voneinander abweichen und unterschiedlich ausgelegt werden, würde dies den Nutzen einer verbesserten Zusammenarbeit zwischen den Datenschutzbehörden schmälern**.

Die erwarteten **finanziellen und wirtschaftlichen Auswirkungen dieser Option sind begrenzt,** die ermittelten Probleme würden weitgehend bestehen bleiben.

6.2. Option 2: Aktualisierung der Regelung

Die **Rechtsunsicherheit wird** für Privatunternehmen und Behörden **erheblich abnehmen**. Problematische Bestimmungen werden klargestellt. Durch eine Einschränkung des Auslegungsspielraums sowie durch Durchführungsmaßnahmen und/oder delegierte Rechtsakte der Kommission wird die Kohärenz erhöht.

Indem die allgemeine Meldung der Verarbeitung personenbezogener Daten durch ein vereinfachtes **harmonisiertes „Dokumentierungssystem"** ersetzt und die Vorabkontrolle bei sensiblen Daten und einer risikobehafteten Datenverarbeitung beibehalten wird, fällt eine Pflicht der für die Datenverarbeitung Verantwortlichen weg, die derzeit uneinheitlich umgesetzt wird. Die Einhaltung der Vorschriften kann leichter gewährleistet und nachgewiesen werden, wenn die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter durch die Ernennung von Datenschutzbeauftragten – in bestimmten Fällen und mit klar definierten, gezielten Kriterien –, die Einführung von Datenschutz-Folgenabschätzungen und des Grundsatzes des Datenschutzes durch Technik mehr Verantwortung erhalten.

Durch eine EU-weit einheitliche, klare und vereinfachte Regelung und durch die Einführung einer zentralen Anlaufstelle für die Überwachung des Datenschutzes wird der Binnenmarkt gestärkt, wozu auch die Angleichung der Verwaltungsformalitäten der Datenschutzbehörden beiträgt. Allein durch die daraus resultierende Verminderung des Verwaltungsaufwands können jährlich rund **2,3 Mrd. EUR eingespart** werden.

Eine einheitlichere Durchsetzung wird auch dadurch gewährleistet, dass die Datenschutzbehörden mehr und einheitlichere Befugnisse erhalten, ein solides Verfahren für Zusammenarbeit und gegenseitige Amtshilfe für Fälle mit einer EU-Dimension eingeführt wird und die administrativen Strafen harmonisiert werden.

Eine **EU-weit harmonisierte Pflicht zur Meldung von Datenschutzverstößen** wird den Einzelnen besser schützen, sektorübergreifend für Kohärenz sorgen und Wettbewerbsnachteile vermeiden.

Die Rechte der Betroffenen und die Kontrolle des Einzelnen über seine Daten würden durch die Einführung neuer Rechte sowie durch die Verbesserung und Klärung der bestehenden Rechte **erheblich gestärkt**. Kinder werden durch spezielle Bestimmungen besonders geschützt. Die Handhabe der Verbände, was die Unterstützung von Betroffenen bei der Wahrnehmung ihrer Datenschutzrechte allgemein und vor Gericht anbelangt, wird gestärkt.

Die **Anwendung allgemeiner Datenschutzgrundsätze auf die Bereiche der polizeilichen und der justiziellen Zusammenarbeit in Strafsachen** würde den EU-Datenschutzrahmen insgesamt kohärenter machen, ohne die Besonderheiten der Strafverfolgung außer Acht zu lassen. Die Rechte des Einzelnen würden vor allem dadurch gestärkt, dass auch die inländische Verarbeitung in den Geltungsbereich der einschlägigen Datenschutzregeln einbezogen wird, indem Bedingungen für das Auskunftsrecht festgelegt und strengere Regeln für die Zweckbindung vorgegeben werden.

Die **finanziellen und wirtschaftlichen Kosten,** die mit der Verpflichtung größerer Unternehmen (mit mehr als 250 Angestellten) zur Benennung eines Datenschutzbeauftragten verbunden sind, **werden nicht unverhältnismäßig sein**, da sehr viele dieser Unternehmen bereits Datenschutzbeauftragte haben. Die Kosten der Einhaltung würden 320 Mio. EUR pro Jahr betragen. Diese Pflicht würde für die erforderliche Mindestzahl von für die Datenverarbeitung Verantwortlichen gelten, da KMU in der Regel von dieser Pflicht ausgenommen sind, es sei denn, deren Datenverarbeitungsaktivitäten sind mit erheblichen Datenschutzrisiken verbunden. Behörden und andere öffentliche Stellen könnten je nach Organisationsstruktur für mehrere Einrichtungen einen gemeinsamen Datenschutzbeauftragten bestellen (z. B. für mehrere Zweigstellen, Abteilungen, Dienststellen).

Die Vereinfachung der Regeln für den internationalen Datentransfer (beispielsweise die Ausweitung des Geltungsbereichs verbindlicher unternehmensinterner Vorschriften) würde sich auch positiv auf die Wettbewerbsfähigkeit der EU-Unternehmen auf dem Weltmarkt auswirken.

Allerdings wäre die Stärkung der Befugnisse und der Unabhängigkeit der Datenschutzbehörden in Verbindung mit der Verpflichtung der Mitgliedstaaten, ausreichende Mittel zur Verfügung zu stellen, für die Behörden, die zur Zeit noch keine ausreichenden Befugnisse und Mittel haben, mit Zusatzkosten verbunden.

Zudem entstehen den nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten (EDSB) durch das neue Verfahren für Zusammenarbeit und gegenseitige Amtshilfe für die Datenschutzbehörden Zusatzkosten. So würden die zusätzlichen Aufgaben des EDSB**,** der die Sekretariatsaufgaben des die Artikel-29-Datenschutzgruppe der EU ersetzenden Europäischen Datenschutzausschusses wahrnehmen soll, insbesondere seine Aufgabe im Kohärenzverfahren eine jährliche Aufstockung seiner Mittel – darunter der Mittel für zusätzliches Personal (10 zusätzliche VZE) – um durchschnittlich 3 Mio. EUR in den ersten sechs Jahren erfordern.

6.3. Option 3: Detaillierte Rechtsregelung auf EU-Ebene

Durch präzisere, sektorspezifische Bestimmungen, die die in Option 2 dargelegten Maßnahmen umfassen, aber darüber hinausgehen, ließen sich die **Unterschiede zwischen den Mitgliedstaaten weitestgehend beseitigen**. Allerdings hätten die Mitgliedstaaten unter Umständen zu wenig Spielraum zur Berücksichtigung ihrer nationalen Gegebenheiten.

Die völlige Abschaffung der Meldepflicht – außer bei Vorabkontrollen – würde das Regelungsumfelds erheblich vereinfachen und den Verwaltungsaufwand verringern.

Die Einrichtung einer Europäischen Datenschutzbehörde würde die **Durchsetzung** wesentlich **kohärenter** machen und in Fällen mit klarer EU-Dimension Unstimmigkeiten beseitigen, doch könnten die Befugnisse einer solchen EU-Behörde den Rahmen des EU-Rechts sprengen. Diese Option käme der EU jedoch sehr teuer. Harmonisierte strafrechtliche Sanktionen würden ebenfalls eine kohärente Durchsetzung fördern. Jedoch kann davon ausgegangen werden, dass die Mitgliedstaaten dies entschieden ablehnen.

Die Rechte der betroffenen Personen, darunter auch die Rechte der Kinder, würden beispielsweise durch die Erweiterung der Begriffsbestimmung von sensiblen Daten um die Daten von Kindern, biometrische und finanzielle Daten gestärkt werden. Durch die

Einführung des Rechts auf Verbandsklagen könnte die Rechtsdurchsetzung vor Gericht maximale Wirkung erhalten. Zudem verspräche eine Harmonisierung der Sanktionen, darunter auch der strafrechtlichen Sanktionen, auf EU-Ebene auch eine Stärkung der Rechte des Einzelnen.

Eine explizite Änderung aller Instrumente im Sinne einer Ausdehnung der allgemeinen Datenschutzregeln auf den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen würde sich positiv auf die Kohärenz der Regeln in diesem Bereich und auf die Rechte des Einzelnen auswirken. Ein solch tiefgreifender Ansatz träfe jedoch bei den Mitgliedstaaten auf Widerstand und wäre politisch schwer durchsetzbar.

7. VERGLEICH DER OPTIONEN

Option 1 wäre mit geringen Einhaltungs- und Verwaltungskosten verbunden, besonders für die Verantwortlichen für die Verarbeitung in der Privatwirtschaft, da die Zusatzkosten größtenteils von nationalen Behörden und Behörden der EU zu tragen wären. Jedoch wären auch die **positiven Auswirkungen begrenzt**: **nur schwer ließen sich Probleme ermitteln und Ziele erreichen**.

Was die politische Durchsetzbarkeit anbelangt, dürfte diese – in keiner Weise kontroverse – Option bei den interessierten Kreisen wegen der begrenzten Reichweite und Wirkung auf Widerstand stoßen und würde als nicht ehrgeizig genug betrachtet werden.

Option 2 wird die **Unterschiede beim Datenschutz und die Rechtsunsicherheit erheblich verringern**. Sie wäre wesentlich wirksamer, was die Ermittlung von Problemen und die Erreichung von Zielen anbelangt. **Die mit dieser Option verbundenen Kosten der Einhaltung dürften angesichts des Nutzens und der Einsparungen beim Verwaltungsaufwand in Höhe von mehr als 2,3 Mrd. EUR pro Jahr verhältnismäßig sein. Und das ist für Unternehmen sehr wichtig**. Diese Option wird insgesamt zu einer besseren und einheitlicheren Durchsetzung führen. Die Abschaffung der Meldepflicht zugunsten eines viel weniger aufwendigen einfachen Dokumentierungssystems würde zudem das Regelungsumfeld vereinfachen und die Verwaltungslast verringern.

Was die Akzeptanz durch die interessierten Kreise anbelangt, würde diese Option von den Unternehmen und Behörden allgemein begrüßt werden, da die Kosten der Einhaltung, insbesondere die durch die derzeitigen unterschiedlichen Regelungen bedingten Kosten, insgesamt sinken werden. Die Interessengruppen, die sich für den Datenschutz einsetzen, insbesondere die Datenschutzbehörden, würden die Stärkung der Datenschutzrechte befürworten. Hinsichtlich des dritten allgemeinen Ziels würde diese Option durch die Aufhebung und „Lissabonnisierung“ des Rahmenbeschlusses und durch die Schließung von Lücken, insbesondere durch die Einbeziehung der innerstaatlichen Verarbeitung in die Regelung, helfen, das Ziel **kohärenterer Datenschutzbestimmungen im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zu erreichen**.

Option 3 umfasst die meisten Maßnahmen der Option 2, geht aber in mehreren Punkten viel weiter. Sie hätte daher **infolge der Senkung der durch die unterschiedlichen Rechtsregelungen bedingten Kosten und der Stärkung der Rechte des Einzelnen eine durchschlagende positive Auswirkung**. Zudem würde eine optimale Kohärenz der Datenschutzregeln in der ehemaligen dritten Säule erreicht und der Datenschutz in diesem Zusammenhang erhöht. Einige der Maßnahmen dieser Option wären jedoch mit

übermäßigen Einhaltungskosten verbunden oder werden aller Wahrscheinlichkeit nach bei den interessierten Kreisen auf starken Widerstand stoßen. Darüber hinaus wäre es sehr schwierig und politisch umstritten, alle Instrumente der ehemaligen dritten Säule gleichzeitig ändern zu wollen.

Bevorzugte Option:

Die ***bevorzugte Option*** ist Option 2 in Verbindung mit folgenden Maßnahmen:

– Abschaffung der Meldepflicht, wie in Option 3 vorgesehen, und

– einige „weiche" Maßnahmen der Option 1: Förderung von Technologien zum Schutz der Privatsphäre und Einführung der Zertifizierung sowie Sensibilisierungskampagnen

Mit der bevorzugten Option dürften sich die politischen Ziele ohne übermäßige Einhaltungskosten und mit erheblich reduziertem Verwaltungsaufwand am ehesten erzielen lassen.

Die verstärkten Datenschutzregeln dürften mit einigen Zusatzkosten für die Einhaltung verbunden sein, besonders wenn es sich um für eine risikobehaftete Datenverarbeitung Verantwortliche handelt. Jedoch kann eine starke Datenschutzregelung der Wirtschaft der EU einen Wettbewerbsvorteil bringen, da der bessere Datenschutz und der erwartete Rückgang von Datenschutzverletzungen das Vertrauen der Verbraucher stärken können. Wenn Unternehmen gezwungen werden, strenge Datenschutzstandards einzuführen, kann dies langfristig für europäische Unternehmen positiv sein: sie könnten bei Technologien zum Schutz der Privatsphäre oder Lösungen des integrierten Datenschutzes eine Führungsposition auf dem Weltmarkt erringen und Unternehmen, Arbeitsplätze und Kapital anziehen.

Darüber hinaus wird eine verstärkte Harmonisierung die grenzüberschreitende Verarbeitung personenbezogener Daten vereinfachen und billiger machen. Dadurch dürften die betreffenden Unternehmen erheblichen Anreiz haben, sich die Vorteile des Binnenmarktes zunutze zu machen und ins Ausland zu expandieren, was sowohl für Verbraucher als auch für die europäische Wirtschaft insgesamt von Nutzen wäre.

Die bevorzugte Option bietet auch eine ausgewogene Lösung für das Problem 3, da sie die Rechte des Einzelnen stärkt, Lücken schließt und Unvereinbarkeiten beim Datenschutz im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen beseitigt und gleichzeitig die Zusammenarbeit bei der Rechtsdurchsetzung verbessert. Dabei werden auch die Besonderheiten dieses Bereichs und der operative Bedarf berücksichtigt.

8. MONITORING UND EVALUIERUNG

Beim Monitoring und bei der Evaluierung der Auswirkungen der bevorzugten Option werden Elemente wie die Verwendung neuer, durch die Reform eingeführter Instrumente, die Befugnisse und Ressourcen der nationalen Datenschutzbehörden, die Sanktionen bei einer Verletzung von Datenschutzvorschriften, der Zeitaufwand und die Kosten der Einhaltung durch die für die Verarbeitung Verantwortlichen sowie der Aufbau von Vertrauen in den Schutz personenbezogener Daten im Internet im Mittelpunkt stehen.