ZUSÄTZLICHE ANMERKUNGEN DES EDSB ZUM DATENSCHUTZREFORMPAKET

I. ANONYMISIERUNG UND PSEUDONYMISIERUNG

1. Konzepte

1. Es wurden zahlreiche Änderungen zur Definition der Begriffe Anonymisierung und Pseudonymisierung und zur Einführung spezifischer Regeln im Hinblick auf Daten vorgeschlagen, die auf diese Weise bearbeitet werden[1]. Obgleich ausgewogenene Maßnahmen Anreize schaffen *können*, um die Verwendung dieser Techniken zur Verbesserung des Datenschutzes zu fördern, könnten zu breit angelegte Ausnahmen zur Aufweichung des alteingeführten Konzeptes der personenbezogenen Daten führen, so wie dies in der Richtlinie 95/46/EG definiert wurde. **Nach Ansicht des EDSB sollte sichergestellt werden, dass die Abänderungen bezüglich der Definition anonymer und pseudonymer Daten der Begriffsbestimmung der personenbezogenen Daten voll und ganz gerecht werden und nicht zu einer ungebührlichen Streichung bestimmter Datenkategorien aus dem Anwendungsbereich der Verordnung führen, insbesondere in Fällen, in denen nicht klar ist, ob die Daten tatsächlich vollständig anonymisiert wurden. In diesen Fällen sollten die Daten weiterhin in den Anwendungsbereich der Verordnung fallen.**

2. Insbesondere sollten bestimmte Kategorien von Daten, die nicht unwiderruflich *anonymisiert* werden, nicht aus dem Anwendungsbereich der Verordnung oder einiger der darin enthaltenen Grundsätze ausgeschlossen werden. Der EDSB mahnt auch zur Vorsicht im Hinblick auf diejenigen Änderungen, in denen Pseudonymisierung mit Anonymisierung verwechselt wird und folglich *pseudonymisierte* Daten aus dem Anwendungsbereich der Verordnung oder deren Hauptgrundsätzen ausgeschlossen werden. Insbesondere:
    - LIBE-Abänderungen 729, 730 und andere ähnlich lautende Abänderungen, die davon ausgehen, dass eine Definition von „pseudonymen“ oder „pseudonymisierten“ Daten mit einigen Berichtigungen der Sprache annehmbar wären, was unseren in Punkt 2 unten enthaltenen Anmerkungen entspricht.
    - Der EDSB spricht sich gegen LIBE AM 726 und 728 aus.
    - Abänderungen, durch welche die Pseudonymisierung ein ausreichender Grund für die Rechtmäßigkeit der Datenverarbeitung wäre, wie LIBE AM

[1] In einigen Fällen wird auch die Verschlüsselung auf ähnliche Weise betrachtet, obgleich dies eine völlig andere technische Maßnahme darstellt, die nur eine beschränkte Wirkung hat, insbesondere auf die Datensicherheit.

Postanschrift: rue Wiertz 60 - 1047 Brüssel, Belgien
Dienststelle: rue Montoyer 30
E-Mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 – Fax: +32 (0)2 283 19 50

887, 897, 898, 900, oder die eine Profilierung mit solchen Daten zulassen, z. B. LIBE AM 1568, 1585 sollten **zurückgewiesen** werden.

2. Begriffsbestimmungen

3. Die Bestimmung des Begriffs „personenbezogene Daten" ist in Artikel 2 Absatz a der Richtlinie 95/46/EG (in Verbindung mit Erwägungsgrund 26) enthalten. Außerdem hat die Artikel-29-Arbeitsgruppe Richtlinien zum Begriff der personenbezogenen Daten zur Verfügung gestellt[2], wobei eine Reihe von Kriterien herausgearbeitet wurden, die dabei behilflich sind, festzustellen, ob die Definition zutrifft. Das wesentliche Kriterium ist das der **Bestimmbarkeit** der natürlichen Person. Dieses Kriterium prüft zwei Elemente:

   a) ob die natürliche Person *direkt* oder *indirekt* identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind (Artikel 2 Absatz a der Richtlinie) und
   b) *im Hinblick auf wen*: den für die Verarbeitung Verantwortlichen, den Auftragsverarbeiter und einen etwaigen Dritten, der angemessene Mittel einsetzt, um diese natürlichen Personen zu identifizieren (Erwägungsgrund 26 der Richtlinie).

4. Außerdem sei angemerkt, dass – aufgrund des technologischen Fortschritts – die Mittel, die der für die Verarbeitung Verantwortliche oder ein Dritter einsetzen könnte, um eine natürliche Person zu identifizieren, seit 1995 zugenommen haben. Es wird erwartet, dass dieser Trend in der Zukunft anhält.

5. Die **Anonymisierung** personenbezogener Daten bedeutet eine Änderung eines Datensatzes, damit es für den für die Verarbeitung Verantwortlichen oder für jeden anderen unmöglich wird, die Person, auf die sich die Daten beziehen, direkt oder indirekt zu bestimmen. **Anonyme Daten sind keine personenbezogenen Daten und fallen nicht in den Anwendungsbereich der Datenschutzbestimmungen.** Die Anonymisierung setzt nicht nur das Löschen aller direkt identifizierenden Attribute (z. B. Namen, Nummern in Zivilregistern, Telefonnummern, biometrische Daten) aus dem Datensatz voraus, sondern in der Regel auch von Daten, die - miteinander kombiniert - einzigartige Merkmale erkennbar machen und alle weiteren Änderungen[3], um einer Rückidentifizierbarkeit vorzubeugen. Einige Arten personenbezogener Daten, wie die biometrischen Daten, sind für sich genommen schon ausreichend, um betroffene Personen zu identifizieren und können folglich aufgrund ihrer Art (z. B. Gesichtsaufnahmen, Fingerabdrücke) nicht Teil eines anonymisierten Datensatzes sein. Jüngste Studien deuten darauf hin, dass auch feinkörnige Standortdaten ausreichend sein könnten, um die Person zu identifizieren, auf welche sich die Daten beziehen. Das Konzept der Identifizierung umfasst außerdem die Möglichkeit, eine Person von anderen Personen zu

[2] Stellungnahme der Artikel-29-Arbeitsgruppe 4/2007 zum Begriff „personenbezogene Daten", WP 136, 20.6.2007.

[3] Wenn Daten eine ausreichende Anzahl von Attributen enthalten, ist die Wahrscheinlichkeit hoch, dass natürliche Personen eine einzigartige Kombination von Werten besitzen und bestimmt werden können. Forschungsarbeiten haben ergeben, dass selbst statistische Datensätze rückidentifiziert werden können, sofern keine spezifischen Maßnahmen ergriffen werden, um dies zu vermeiden. Siehe beispielsweise: http://www.census.gov/srd/papers/pdf/rrs2012-13.pdf

unterscheiden („Aussonderung"), selbst wenn keine gemeinhin verwendeten Kennzeichen verfügbar sind.

6. Auf der anderen Seite beziehen sich **pseudonymisierte Daten** per Definition auf eine bestimmbare natürliche Person, da die Beziehung zwischen dem Pseudonym und den Identifizierungsdaten (d. h. Vorname und Name, Anschrift, etc.) dem für die Verarbeitung Verantwortlichen oder einem Dritten bekannt sind. Selbst wenn das Pseudonym und dessen Korrelation mit der Identität ausschließlich einer einzigen gegebenen Partei bekannt sind (ganz gleich, ob es sich dabei um den für die Verarbeitung Verantwortlichen oder einen vertrauenswürdigen Dritten handelt) und nicht mit anderen geteilt werden, **bleiben pseudonymisierte Daten personenbezogene Daten**[4]. **Pseudonymisierte Daten fallen folglich in den Anwendungsbereich der Verordnung**[5].

7. Unter Berücksichtigung dieser Überlegungen schlägt der EDSB vor, dass jede Definition des Begriffs „Pseudonym" auf folgenden Elementen basiert:

   - „pseudonymisierte Daten" sind Informationen im Zusammenhang mit einer natürlichen Person, die direkt oder indirekt bestimmt werden kann (d. h. diese Daten fallen weiterhin unter den Begriff „personenbezogene Daten"),
   - die Mittel, die eingesetzt werden können, um die Person zu identifizieren, sind effektiv von den betroffenen Daten getrennt und
   - die Identifizierung durch Unbefugte wird effektiv verhindert.

3. Folgen für weitere Teile des Vorschlags

8. Da **pseudonyme Daten personenbezogene Daten bleiben,** spricht sich der EDSB gegen Abänderungen aus, die vorsehen, dass auf die Verarbeitung pseudonymer Daten die wesentlichen Datenschutzgrundsätze, wie Transparenz, Rechtmäßigkeit der Verarbeitung und Rechte der betroffenen Personen, keine Anwendung finden. Gleichzeitig könnte die Verordnung Anreize für eine Verarbeitung pseudonymer Daten im Guten Glauben seitens der für die Verarbeitung Verantwortlichen oder der Auftragsverarbeiter enthalten, vorausgesetzt, die Verarbeitung entspricht strengen Bedingungen (z. B. zur Sicherheit und Geheimhaltung). Dies könnte beispielsweise im Kontext der Bestimmungen zur Verletzung des Schutzes personenbezogener Daten (Artikel 31 und 32) vorkommen, je nachdem, ob die von der Verletzung des Schutzes betroffenen Daten angemessen vor einer

[4] Datensätze, die keine gemeinen identifizierenden Attribute enthalten (wie den Namen und die Anschrift), sondern eindeutige Werte, die in Transaktionen mit vielen Parteien verwendet werden (wie IP-Adressen oder Cookie-Nummern) können noch nicht einmal als pseudonym betrachtet werden, da viele Dritte Kenntnis von diesen Attributen haben und in der Lage sein können, die betroffene Person zu bestimmen. In diesem Fall sind die Daten personenbezogene Daten, die identifizierbar sind, „mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung ...".

[5] Eine ganz andere Technik ist die der Verschlüsselung, d. h. das technische Verfahren, mit dem Daten vorübergehend in eine nichtlesbare oder unverständliche Form zu Zwecken der Vertraulichkeit oder der Unversehrtheit verschlüsselt werden, so dass Eindringlinge oder Hacker diese nicht lesen oder ändern können, während die befugten Nutzer dies können. Verschlüsselte personenbezogene Daten sollten nicht als anonymisierte Daten betrachtet werden, da die Verschlüsselung nur vorübergehender Natur ist und jeder, der in Besitz des Schlüssels des Verschlüsselungsverfahrens ist, die Daten leicht entschlüsseln kann und da die Verschlüsselung mit ausreichenden Mitteln auch ohne eine Schlüssel aufgelöst werden kann. Dennoch kann eine starke und aktualisierte Verschlüsselung das Risiko (und die Folgen) einiger Datenverletzungen beachtlich reduzieren und sollte folglich als wichtige Sicherheitsmaßnahme (z. B. in Artikel 30) anerkannt und gefördert werden, sofern sie angemessen angewandt wird.

Identifizierung geschützt wurden, oder auch bei Bestimmungen im Bereich der Forschung und Statistik (Artikel 83). Dies könnte auch im Hinblick auf den Aufbau neuer IT-Systeme erwägt werden (Artikel 23 zum Datenschutz durch Technik).

II. ANWENDUNGSBEREICH DER VERORDNUNG

1. Materieller Anwendungsbereich

9. Im Hinblick auf den materiellen Anwendungsbereich der Verordnung stellt der EDSB mit Bedenken einen Trend fest, der anhand verschiedener Abänderungen des **Artikels 2** erkennbar ist, wodurch der Anwendungsbereich der zukünftigen Verordnung eingeschränkt wird, indem für spezifische Sektoren oder spezifische Verarbeitungssituationen Ausnahmen vorgesehen werden (z. B. für den Finanzsektor oder den Beschäftigungskontext). Obgleich der EDSB anerkennt, dass in bestimmten Fälle Sonderregelungen ihre Berechtigung haben, stellt er auch fest, dass viele dieser Fälle bereits unter Kapitel IX „Vorschriften für besondere Datenverarbeitungssituationen" fallen. Eine Reihe von Ausnahmen für spezifische Zwecke ist außerdem bereits in Artikel 21 definiert, in dem die Bedingungen enthalten sind, die jede Beschränkung von Rechten und Pflichten gemäß der Verordnung erfüllen muss. Das Hinzufügen weiterer Ausnahmen in Artikel 2 würde nicht nur zu wesentlichen Lücken im Hinblick auf den Schutz der Grundrechte der Unionsbürger führen, sondern stünde sogar im Widerspruch zum Gedanken eines einzigen (möglichst umfassenden und einheitlichen) Rechtsrahmens für den Datenschutz in Europa. Aus diesem Grund spricht sich der EDSB gegen diese Ausnahmen aus.

a) Organe und Einrichtungen der EU

10. Der EDSB stellt fest, dass es eine Reihe von Abänderungen gibt (z. B. LIBE AM 666), welche beabsichtigen, die in Artikel 2 vorgesehene Ausnahme für EU-Organe zu streichen, weshalb Organe, Einrichtungen, Ämter und Agenturen in den Anwendungsbereich der künftigen Verordnung fallen würden.

11. Diese Abänderungen entsprechen den früheren Empfehlungen des EDSB[6] und sind grundsätzlich zu begrüßen. Gleichzeitig sollte jedoch unterstrichen werden, dass – angesichts des spezifischen rechtlichen und institutionellen Rahmens, in denen diese tätig sind – **mehr als eine einfache Streichung der in Artikel 2 vorgesehenen Ausnahme erforderlich ist**, um einen kohärenten Rechtsrahmen und eine hinreichende Rechtssicherheit für alle betroffenen Akteure zu schaffen. Die Verordnung (EG) Nr. 45/2001, die derzeit auf Organe und Einrichtungen der EU anwendbar ist, deckt in der Tat einige Fragen ab, die speziell auf den institutionellen Kontext der EU ausgerichtet sind und die im Rahmen der vorgeschlagenen allgemeinen Verordnung ungeregelt bleiben würden. Diese umfassen: i) die Übermittlung personenbezogener Daten zwischen Organen der EU sowie zwischen diesen Organen und anderen Empfängern; ii) Vorschriften im Hinblick auf die Datenverarbeitung in internen Telekommunikationsnetzwerken[7]; iii) Vorschriften bezüglich der Ernennung des Europäischen

[6] Siehe Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket, Punkte 29-31.

[7] Diese Vorschriften entsprechen im Großen und Ganzen denjenigen der Richtlinie 97/66/EG, die in der Folge überarbeitet und durch die Datenschutzrichtlinie 2002/58/EG für die elektronische Kommunikation ersetzt wurde.

Datenschutzbeauftragten und des stellvertretenden Datenschutzbeauftragten und iv) eine detaillierte Aufstellung der Pflichten und Befugnisse des EDSB, die sich nicht vollständig mit denjenigen der nationalen Aufsichtsbehörden überschneiden und sich auch nicht vollständig überschneiden können, da diese z. B. auch die Beziehung zwischen dem EDSB und dem Gerichtshof der Europäischen Union regeln.

12. Der EDSB spricht sich folglich gegen die einfache Streichung der Ausnahme von Artikel 2 aus, ohne dass im weiteren Text auf die obigen Fragen eingegangen wird, und würde es zumindest wärmstens begrüßen, wenn in einem Erwägungsgrund unterstrichen würde, dass es erforderlich ist, den Rechtsrahmen des Datenschutzes für die Organe und Einrichtungen der EU der Verordnung anzupassen, sobald diese anwendbar wird[8].

b) Gerichte in ihrer gerichtlichen Eigenschaft

13. Was die Abänderungen bezüglich des Anwendungsbereichs der Aufsichtsbefugnisse der nationalen Datenschutzbehörden (Artikel 51 der vorgeschlagenen Verordnung) angeht, begrüßt der EDSB diejenigen, die es den Mitgliedstaaten gestatten würden, diese Bestimmungen auch auf die Verarbeitungen der Gerichte auszudehnen, sofern diese in ihrer gerichtlichen Eigenschaft tätig werden (LIBE AM 2595). Dies ist nicht nur mit dem Übereinkommen 108 und dessen Protokoll über die unabhängige Aufsicht vereinbar, sondern auch mit der Tradition verschiedener Mitgliedstaaten und sollte unterstützt werden. Diese Schlussfolgerung basiert auch auf der Tatsache, dass die derzeitige Beschränkung im Vorschlag der Kommission für Staatsanwaltschaften ebenfalls nicht gilt.

2. Einschränkung *rationae temporis*

14. Der EDSB ist der Ansicht, dass die zeitliche Einschränkung der Anwendung der Verordnung (wie z. B. in LIBE AM 664 und 665 vorgesehen) nicht erforderlich ist, da die vorgeschlagene Legisvakanz (zwei Jahre) ausreichend zu sein scheint, um alle bestehenden Verarbeitungen den neuen Bestimmungen anzupassen. Der EDSB spricht sich gegen diese Abänderungen aus.

3. Räumlicher Anwendungsbereich

15. Was den räumlichen Anwendungsbereich angeht, wurden einige Abänderungen im Hinblick auf Artikel 3 Absatz 1 vorgelegt, wonach eine Beschränkung der betroffenen Personen vorgesehen werden und nur diejenigen unter die Verordnung fallen würden, die „**in der Union ansässig sind**“ (LIBE AM 700, LIBE AM 701, LIBE AM 703).

16. Würden diese Abänderungen angenommen, würden sie große Gruppen von betroffenen Personen des Schutzes berauben, den diese heute unter der Richtlinie 95/46/EG genießen. Dazu zählen z. B. Touristen sowie Verarbeitungen, die in der EU im Hinblick auf im Ausland ansässige betroffene Personen durchgeführt werden, was innerhalb der Union zur Schaffung eines doppelten Rechtsstandards führen würde. Außerdem sollte festgestellt werden, dass diese Einschränkung im Sekundärrecht nicht mit dem Primärrecht vereinbar ist, insbesondere mit Artikel 16

[8] Siehe Artikel 91 Absatz 1 des Vorschlags der Kommission.

AEUV und mit Artikel 8 der Charta der Grundrechte der Europäischen Union, die das Recht auf Schutz der personenbezogenen Daten explizit auf „jede Person" ausdehnen, d. h. jede Person, die in den Anwendungsbereich des EU-Rechts fällt, ungeachtet des Ortes, an dem sie ansässig ist. Dies war auch ein wichtiger Ausgangspunkt der Diskussionen mit Drittländern. Angesichts der Tatsache, dass die vorgeschlagene Verordnung den Anwendungsbereich der subjektiven Rechte angemessen einschränkt, **spricht sich der EDSB gehen diese Abänderungen aus**.

III. ZWECKBINDUNG UND RECHTMÄSSIGKEIT DER VERARBEITUNG

1. Zweckbindung

17. Der EDSB begrüßt insbesondere die Abänderung LIBE AM 103, in der vorgeschlagen wird, **Artikel 6 Absatz 4 zu streichen**, wie von der Kommission vorgeschlagen wurde. **Artikel 6 Absatz 4** eröffnet die Möglichkeit, Daten zu unvereinbaren Zwecken zu verarbeiten, solange eine Rechtsgrundlage in Artikel 6 Absatz 1 Buchstaben a bis e gegeben ist. Dieser Text würde in Wirklichkeit bedeuten, dass es jederzeit möglich wäre, den Mangel an Vereinbarkeit zu überwinden, indem einfach eine neue Rechtsgrundlage für die Verarbeitung identifiziert wird. Der EDSB unterstreicht jedoch[9], dass das Verbot der unvereinbaren Nutzung und die Anforderung der Rechtmäßigkeit kumulative Anforderungen sind. Das Erfordernis der Vereinbarkeit kann nicht einfach durch Verweis auf eine Bedingung der Rechtmäßigkeit der Verarbeitung aufgehoben werden. Dies wäre nicht mit Artikel 5 des Übereinkommens 108 des Europarates vereinbar, das für alle Mitgliedstaaten verbindlich ist.

18. Die Logik der Richtlinie 95/46/EG besagt, dass eine solche unvereinbare Nutzung nur zulässig ist, wenn die Bedingungen von Artikel 13 für bestimmte Gründe öffentlichen Interesses erfüllt sind (siehe Artikel 21 der vorgeschlagenen Verordnung). Folglich **unterstützt der EDSB die Streichung von Artikel 6 Absatz 4**, was die Logik der Richtlinie 95/46/EG wahren würde (während eine Änderung des Zweckes unter strengen Bedingungen gemäß Artikel 21 möglich wäre). Die Frage der Vereinbarkeit ist eine Schlüsselfrage, zu der die Artikel-29-Arbeitsgruppe in den nächsten Wochen eine Stellungnahme annehmen wird. Diese Stellungnahme wird wesentliche Leitlinien und Kriterien für ein gemeinsames Verständnis des Begriffs „Vereinbarkeit" enthalten.

19. Der EDSB spricht sich gegen Abänderungen aus, die dafür sprechen, dass die weitere Verarbeitung von Daten zu gesundheitlichen Zwecken nicht als unvereinbar betrachtet werden sollte (LIBE AM 821), da die weitere Verarbeitung dieser sensiblen Daten wesentliche Auswirkungen auf den Schutz der Privatsphäre natürlicher Personen haben kann. Gemäß geltendem Recht hängt die Möglichkeit zur weiteren Verarbeitung von Kriterien, wie den gerade genannten, ab.

2. Rechtmäßigkeit der Verarbeitung

20. Der Entwurf des LIBE-Berichts schlägt lange vorschreibende Listen für **Artikel 6 Absatz 1 Buchstabe b und Artikel 6 Absatz 1 Buchstabe c** vor, die beschreiben, in welchen Situationen die berechtigten Interessen der für die Verarbeitung

[9] Vgl. auch die Stellungnahme des EDSB vom 7. März 2012, Punkte 115-124.

Verantwortlichen die Rechte und Interessen der betroffenen Personen aufheben und umgekehrt (LIBE AM 99-102). **Nach Ansicht des EDSB sind diese vorschreibenden Listen kontraproduktiv und sollten zurückgewiesen werden.**

21. Der EDSB empfiehlt, dass diese Listen durch eine prägnantere Bestimmung ersetzt werden, wobei berücksichtigt wird, dass es viele Situationen gibt, die nicht vorhergesehen werden können und ganz konkret im Einzelfall geprüft werden müssen. Außerdem könnte **ein Erwägungsgrund** die typischsten relevanten Faktoren auflisten, die im Hinblick auf das Gleichgewicht zwischen den zur Rede stehenden Interessen und Grundrechten berücksichtigt werden sollten. Falls erforderlich, können Beispiele dafür aufgeführt werden, was unter „berechtigten Interessen" zu verstehen ist.

22. Im Gegensatz dazu begrüßt der EDSB die vorgeschlagene Abänderung von **Artikel 6 Absatz 1 Buchstabe a** (LIBE AM 100), die zu mehr Transparenz im Hinblick auf die Begründung dafür aufruft, dass „seine berechtigten Interessen Vorrang vor den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person haben". Dies würde für mehr Verantwortlichkeit im Hinblick auf die Art und Weise sorgen, wie ein annehmbares Gleichgewicht der Interessen erzielt werden kann.

23. Abschließend unterstreicht der EDSB, dass das Konzept der **expliziten Einwilligung,** so wie dieses derzeit im Vorschlag der Kommission definiert ist (insbesondere Artikel 4 Absatz 8, Artikel 6 Absatz 1 Buchstabe a und Artikel 7), **beibehalten werden sollte**. Es sorgt für Flexibilität im Hinblick auf die Ausdrucksweise (durch eine Erklärung oder eine bestätigende Handlung) und sieht das Erfordernis einer Einwilligung „ohne jeden Zweifel" vor, was ein wesentliches Element des Gleichgewichts des Datenschutzes seit 1995 insgesamt darstellt. Die EU-Datenschutzbehörden haben die Anforderung gemäß Artikel 7 Buchstabe a der Richtlinie 95/46/EG im Hinblick auf Artikel 2 Buchstabe h einheitlich dahingehend ausgelegt, dass diese Einwilligung „ohne jeden Zweifel" erteilt worden sein muss, was wiederum bedeutet, dass sie „explizit" sein muss[10] (so dass beispielsweise das Unterbleiben einer Handlung oder Stillschweigen nicht als eindeutig betrachtet werden kann). Folglich empfiehlt der EDSB, dass Abänderungen wie ITRE AM 83, IMCO AM 63 und die vorgeschlagenen LIBE AM 757, 758, 760, 764-766, usw., **zurückgewiesen** werden.

IV. ROLLEN, VERANTWORTLICHKEITEN UND HAFTUNG DES FÜR DIE VERARBEITUNG VERANTWORTLICHEN / DES AUFTRAGSVERARBEITERS

24. Abänderungen im Hinblick auf die Rollen des für die Verarbeitung Verantwortlichen/Auftragsverarbeiters sind in vielen Teilen des Textes enthalten, auch in den Begriffsbestimmungen. Mehrere Abänderungen sehen eine Streichung des Konzepts vor, wonach der für die Verarbeitung Verantwortliche **nicht nur die Zwecke sondern auch „die Bedingungen und Mittel"** der Verarbeitung bestimmt, wie in Artikel 4 Absatz 5 des Vorschlags definiert (z. B. ITRE AM 81; IMCO AM 62; LIBE AM 746, 747, 748). Die Kriterien, gemäß welchen der für die

[10] Siehe insbesondere die Stellungnahme der Artikel-29-Arbeitsgruppe 15/2011 zur Definition der Einwilligung, WP 187, 13.7.2011.

Verarbeitung Verantwortliche die „Zwecke und Mittel“ der Verarbeitung bestimmt, sind in der Richtlinie 95/46/EG festgelegt und wurden in der Stellungnahme 1/2010 der WP 29 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ weiterentwickelt. **Diese Kriterien haben effektiv zum Verständnis und der Abgrenzung der Rollen des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters beigetragen und sollten nicht gestrichen werden.**

25. Zahlreiche Abänderungen zielen darauf ab, die im Vorschlag vorgesehenen Verantwortlichkeiten des für die Verarbeitung Verantwortlichen zu schmälern, zum Beispiel, indem die Verpflichtungen des Auftragsverarbeiters im Hinblick auf die Dokumentation, die Durchführung einer Datenschutzfolgenabschätzung oder die Unterstützung des für die Verarbeitung Verantwortlichen im Hinblick auf die Sicherheitsanforderungen gestrichen oder geschwächt werden (wie in ITRE AM 43, 229, 233, 238, 260; LIBE AM 1829, 1832, 1834, 1836, 1837, 2024). Die Ausdehnung bestimmter Verpflichtungen auf die Auftragsverarbeiter spiegelt jedoch die derzeitige Bedeutung der Auftragsverarbeiter bei der Bestimmung wesentlicher Bedingungen der Verarbeitung wider (z. B. im Kontext des Cloud Computing, wo diese häufig über Übermittlungen und die Unterverarbeitung entscheiden). **In diesem Kontext sollten die Auftragsverarbeiter für ihre Verarbeitung verantwortlich gemacht werden.** Die Bestimmung, wonach Auftragsverarbeiter, die keine Anweisungen befolgen oder sich über diese hinwegsetzen, zu einem für die Verarbeitung Verantwortlichen werden (Artikel 26 Absatz 4), sollte beibehalten werden. Der EDSB spricht sich deshalb gegen die in ITRE AM 231 und LIBE AM 1808-1810 enthaltenen Vorschläge aus.

26. Die **drei Bestandteile der Verantwortlichkeit sollten beibehalten werden. Gewährleistung**, **Nachweis** und **Überprüfung der *Compliance***. Verschiedene Abänderungen aus mehreren Ausschüssen, die versuchen, sämtliche oder einige dieser Aspekte der Verantwortlichkeit zu streichen, um so die für die Verarbeitung Verantwortlichen zu entlasten (z. B. ITRE AM 199, 204, 207; LIBE AM 1658, 1661, 1687, 1688, 1834, 1836), sollten zurückgewiesen werden. Auch die Abänderungen, die darauf abzielen, Artikel 28 zur Dokumentation zu streichen (LIBE AM 1825, 1826, 1830), sollten zurückgewiesen werden.

27. Albrecht AM 188 schlägt vor, dass die in Artikel 28 vorgesehene Dokumentation im Wesentlichen dieselbe Information ist, die der betroffenen Person gemäß Artikel 14 erteilt werden muss, um so den Verwaltungsaufwand zu reduzieren. Obgleich dies eine Vereinfachung zu sein scheint, da die in Artikel 28 enthaltene Liste sich in gewissem Maß mit der Liste der den betroffenen Personen gemäß Artikel 14 zur Verfügung zu stellenden Informationen deckt, bestehen Zweifel daran, dass die in Artikel 14 (selbst wenn diese, wie in Albrecht AM 125-133 vorgesehen, erweitert wird) aufgeführte Dokumentation zur Überprüfung der *Compliance* ausreichend ist. Nach Ansicht des EDSB sollten die als Dokumentation geführten Informationen ausreichende Daten enthalten, die auf Anfrage der Aufsichtsbehörden eine Überprüfung der beiden nachfolgend genannten Aspekte im Hinblick auf die Verarbeitungsvorgänge ermöglichen:

    i) sie sollten den Nachweis dafür enthalten, wie das Kontrollsystem der Verarbeitungsvorgänge strukturiert ist und

ii) sie sollten den Nachweis dafür enthalten, wie beide funktionieren (z. B. auf der Grundlage von Logdateien).

28. Abschließend begrüßt der EDSB Abänderungen, die die Maßnahmen eingehender beschreiben, welche die Organisationen intern umsetzen sollten, um ihrer Verantwortlichkeit nachzukommen (wie interne Richtlinien und Verfahren, Weiterbildung des Personals, Nachweise für das Engagements der Führungsebene, Überprüfung der Wirksamkeit in regelmäßigen Abständen, wie in ITRE AM 205, 210, 212, 213; LIBE AM 1684, 1698 vorgesehen).

V. FLEXIBILITÄT, RISIKOORIENTIERTER ANSATZ, KKMU

29. Mehrere Abänderungen zielen darauf ab, einen risikoorientierten Ansatz mittels einer detaillierten Liste einzuführen, in der die riskanten Verarbeitungsvorgänge aufgeführt werden. **Der EDSB spricht sich gegen Abänderungen aus, die dazu führen könnten, dass der Schutz nur im Hinblick auf die riskantesten Verarbeitungsvorgänge Anwendung findet.** Der volle in der Verordnung vorgesehene Schutz sollte für alle Verarbeitungsvorgänge gelten, nicht nur für die mit den größten Risken (zum Beispiel das Prinzip des Datenschutzes durch Technik sollte nicht „bei Bedarf" oder aufgrund eines risikoorientierten Ansatzes gelten, wie in IMCO AM 138 und 140, ITRE 216 vorgesehen). Es sollte berücksichtigt werden, dass jede Datenverarbeitung ein Risiko birgt. Außerdem empfiehlt der EDSB die Zurückweisung von Abänderungen, die das Gleichgewicht zwischen Risiko und Maßnahmen ändern, z. B. im Hinblick auf Artikel 30 zur Sicherheit (ITRE AM 243, LIBE AM 1922, 1923, 1924, 1925, 1926). Das vorgeschriebene Risikomanagement wird die Verhältnismäßigkeit von Aufwand und Risiko gewährleisten.

30. Im Gegensatz dazu **erkennt der EDSB zahlreiche positive Elemente im progressiven risikoorientierten Ansatz, der vom Rat angestrebt wird**[11]. Dieser Ansatz sieht vor, dass detailliertere Verpflichtungen bei höheren Risiken Anwendung finden, während die Vorgaben bei niedrigeren Risiken reduziert werden sollten. Eine horizontale Risikobestimmung würde in Artikel 22 eingeführt und zahlreiche Bestimmungen in Kapitel IV der Verordnung würden neuformuliert werden, um **dem Grundsatz der Rechenschaftspflicht** ein größeres Gewicht zu verleihen. Es wird so versucht, Anreize zu schaffen, um die Verpflichtungen des für die Verarbeitung Verantwortlichen innerhalb von solchen Organisationen zu erleichtern, die Maßnahmen zur Stärkung der Rechenschaftspflicht umgesetzt haben.

31. In diesem Zusammenhang wurden dem Parlament verschiedene Abänderungen vorgelegt, um dem Begriff der Rechenschaftspflicht mehr Gewicht zu verleihen und verschiedene Pflichten des für die Verarbeitung Verantwortlichen zu erleichtern, auch im Hinblick auf die Meldungen an die Aufsichtsbehörden (insbesondere bezüglich Artikel 22-29 und 33-34). **Der EDSB begrüßt die Abänderungen, die den Grundsatz der Rechenschaftspflicht stärken**, da er sich der Notwendigkeit bewusst ist, mehr Flexibilität für diejenigen Organisationen einzuführen, die Mechanismen zur Stärkung der Rechenschaftspflicht eingeführt

[11] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/135901.pdf.

haben, wie die Ernennung eines Datenschutzbeauftragten (DSB) oder die Umsetzung von anerkannten Zertifizierungsmechanismen.

32. Auf der anderen Seite sollte eine Erleichterung bestimmter Pflichten des für die Verarbeitung Verantwortlichen in diesem Kontext nicht zur Streichung wichtiger Pflichten hinsichtlich riskanter Verarbeitungen führen. Der EDSB spricht sich insbesondere gegen Abänderungen aus, die die für die Verarbeitung Verantwortlichen von der Verpflichtung befreien würden, eine Datenschutzfolgenabschätzung durchzuführen, sofern sie einen DSB ernannt haben oder einem Zertifizierungsmechanismus unterliegen (JURI AM 297) oder wenn die Verarbeitung auf einer Einwilligung oder einer rechtlichen Verpflichtung basiert (LIBE AM 2020). In all diesen Fällen sollte bei besonders riskanten Verarbeitungen weiterhin die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung vorgesehen werden, um die Risiken zu bewerten und dadurch zu senken. Außerdem rät der EDSB von Abänderungen ab, die die Verpflichtung der für die Verarbeitung Verantwortlichen, vor Durchführung riskanter Verarbeitungen die Aufsichtsbehörde zu konsultieren, streichen würden (z. B. ITRE AM 207, 208, 272, LIBE AM 2108). **Die Pflicht, der Aufsichtsbehörde Fälle von riskanten Verarbeitungsvorgängen zu melden, sollte fortbestehen, während die Modalitäten des Verfahrens der Meldung bei der Aufsichtsbehörde selbst vereinfacht werden könnten.** So könnten zum Beispiel Anreize für diejenigen Organisationen geschaffen werden, die spezifische Mechanismen zur Gewährleistung der Rechenschaftspflicht verwenden, damit die Meldung in diesem Fall im Rahmen eines zügigen und vereinfachten Verfahrens zur vorherigen Zurateziehung gehandhabt wird, nur um die gute Verfahrenspraxis zu überprüfen.

33. In diesem Zusammenhang ist der EDSB der Ansicht, dass **es mehr Anreize für den Einsatz der Datenschutzbeauftragten geben sollte.** Obgleich bestimmte Verpflichtungen im Hinblick auf riskante Verarbeitungsvorgänge weiterhin auf den für die Verarbeitung Verantwortlichen anwendbar sein sollten, wie die Meldung der Verarbeitung an die Aufsichtsbehörde zur vorherigen Zurateziehung, sollten beispielsweise vereinfachte Verfahren angestrebt werden, sofern ein DSB ernannt wurde, so dass in einem solchen Fall die Verarbeitung ab dem Datum der Meldung beginnt, ohne dass auf eine Antwort der Aufsichtsbehörde gewartet werden muss. Außerdem sollte anerkannt werden, dass jede Organisation Mechanismen zur Wahrung der Datenschutzanforderungen besitzen sollte, was über die Frage hinausgeht, ob die Ernennung eines DSB zwingend vorgeschrieben werden sollte oder nicht. Dies macht es erforderlich, dass verschiedene Personen intern (wie die IT-, Rechts-, Personal- und Compliance-Abteilungen) die *Compliance* der Verarbeitung durch die Organisation mit diesen Anforderungen sicherstellen. In vielen Fällen kann die Beauftragung einer zusätzlichen Person mit der abteilungsübergreifenden Gesamtverantwortung im Hinblick auf Datenschutzfragen sich für die Organisation nicht nur als vorteilhaft, sondern auch als erforderlich erweisen.

34. Mehrere Abänderungen zielen darauf ab, neue Ausnahmen für Kleinst-, Klein- und mittlere Unternehmen einzuführen und sollten zurückgewiesen werden, da sie eine Ausnahme von den allgemeinen Grundsätzen der Verordnung darstellen und nicht nur von spezifischen Bestimmungen. Sie zielen beispielsweise darauf ab, die von KKMU durchgeführte Verarbeitung „zur internen Verwendung“ aus dem

Anwendungsbereich der Verordnung auszuschließen (LIBE AM 678-680) bzw. diese von der Pflicht der Dokumentation gemäß Artikel 28 (z. B. ITRE AM 235) oder von der Durchführung einer Datenschutzfolgenabschätzung zu befreien, insbesondere sofern die Verarbeitung zum *Core Business* des Unternehmens zählt (ITRE AM 160). Ausnahmen oder Einschränkungen im Hinblick auf spezifische Bestimmungen könnten nur in den Fällen angestrebt werden, in denen dies angemessen ist[12].

VI. ÜBERMITTLUNGEN, EINSCHLIESSLICH DER VORGESCHLAGENEN ARTIKEL 43a UND 44a

35. Abänderungen, die darauf abzielen, Elemente des Grundsatzes der „**Angemessenheit**" zu klären oder hinzuzufügen, sollten **zurückgewiesen** werden, da sie lediglich für Verwirrung sorgen könnten (JURI AM 53, LIBE AM 2383 bis 2386).

36. Die Angemessenheit sollte weiterhin für **Bereiche** vorgesehen sein, so wie dies derzeit für bestimmte Angemessenheitsentscheidungen der Fall ist, zum Beispiel Vereinigte Staaten „Sicherer Hafen" (nur im Hinblick auf einige Bereiche des privaten Sektors anwendbar) oder Kanada (nur für den privaten Sektor). Einige Abänderungen des Artikels 41 Absatz 1 streichen diese Möglichkeit (LIBE AM 241). Dies wäre nicht vereinbar mit der Anerkennung des „Grundsatzes der Angemessenheit" als „funktionelles Konzept", um einen bedeutungsvollen Datenaustausch mit Drittländern (oder einem Verarbeitungssektor in einem Drittland) zuzulassen. **Der EDSB spricht sich gegen diese Abänderungen aus.**

37. Auf der anderen Seite war dem Vorschlag der Kommission im Hinblick auf die Übermittlung an Drittländer, deren Schutzniveau nicht als angemessen bezeichnet wurde, nicht eindeutig zu entnehmen, ob Artikel 41 Absatz 5 die Übermittlung an diese Länder insgesamt untersagt oder ob Übermittlungen unter bestimmten Bedingungen möglich wären (Widerspruch zwischen Erwägungsgrund 82 und Artikel 41 Absatz 5). Angesichts dieser Tatsache ist der EDSB der Ansicht, dass positive Änderungen von Artikel 42 Absatz 1 vorgelegt wurden, welche erklären, dass angemessene Garantien in den Fällen eingeführt werden können, in denen die Kommission gemäß Artikel 41 Absatz 5 das Schutzniveau für nicht angemessen erklärt hat (LIBE AM 2415, ITRE AM 305 erster Teil der AM, JURI AM 55). **Diese Abänderungen sollten folglich unterstützt werden.**

38. Der EDSB unterstützt die Abänderungen, welche den **Anwendungsbereich der BCR erweitern** (Artikel 43 Absatz 1 Buchstabe a), damit diese auch **für deren externe Dienstleister** gelten (LIBE 2470 bis 2479). Diese Erweiterung könnte den Schutz verbessern und zur Rechtssicherheit in Bereichen wie dem *Cloud Computing* beitragen, die sich durch eine Vielzahl von Beziehungen mit Dienstleistern auszeichnen.

39. Einige Abänderungen sehen einen neuen **Artikel 43 Buchstabe a zum Datentransfer vor**, **der gemäß EU-Rechtsvorschriften nicht zulässig ist** (Albrecht AM 259, LIBE AM 2490, ebenso JURI AM 354). Der EDSB unterstützt diese Abänderungen, die beispielsweise solche Fälle angehen, in denen ein Antrag

[12] Siehe Stellungnahme des EDSB vom 7. März 2012, Punkte 79-80.

von einem ausländischen Richter (eines Drittlandes) vorliegt, der einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter, die zur Einhaltung der EU-Datenschutzbestimmungen verpflichtet sind, auffordert, personenbezogene Daten zu übermitteln (z. B. E-Discovery-Fälle).

40. Eine andere Abänderung schlägt vor, einen **neuen Artikel 44a** (LIBE AM 2531) bezüglich der Übermittlung an Cloud-Dienste unter der Gerichtsbarkeit von Drittländern einzufügen. In diesem Bereich ist mehr Transparenz in der Tat begrüßenswert. Die Risiken, die mit dieser Abänderung durch die Einführung spezifischer Anforderungen angegangen werden sollen, sind jedoch nicht auf das Cloud-Computing beschränkt, sondern sind typische Risiken internationaler Übermittlungen. Es trifft zu, dass im Bereich des Cloud Computing diese Risiken offensichtlicher sind und dass die Rechte der betroffenen Personen ungewisser sind, da es nicht immer möglich ist, zu wissen, wo die personenenbezogenen Daten sich befinden und welche möglichen Risken in Bezug auf das Bestimmungsland oder die Bestimmungsländer bestehen. Dennoch sollte die Einführung von neuen Anforderungen technisch neutral erfolgen. **Aus diesem Grund spricht sich der EDSB gegen diese Abänderung aus.**

VII. ZUSAMMENARBEIT, KOHÄRENZ, VERBINDLICHE BEFUGNISSE DES EUROPÄISCHEN DATENSCHUTZAUSSCHUSSES

41. Der EDSB begrüßt generell die Einrichtung eines Mechanismus, der eine zentrale Kontaktstelle für die für die Verarbeitung Verantwortlichen vorsieht, die jedoch der „Aufsicht führenden Behörde" keine *exklusive* Befugnis zuerkennt und es folglich betroffenen Personen gestattet, sich an die Aufsichtsbehörde in ihrem Ansässigkeitsstaat zu wenden (Albrecht-Bericht AM 277 zur Einführung eines neuen Artikels 54 Buchstabe a).

42. Der EDSB begrüßt die Abänderungen (des Albrecht-Berichts), in denen die Möglichkeit gestrichen wird, dass die Kommission bei unterschiedlichen Anlässen im Kontext des Kohärenzverfahrens eingreift und eine Entscheidung einer nationalen Aufsichtsbehörde in einer spezifischen Frage aufhebt (wie in Artikel 58, Artikel 59, Artikel 60 Absatz 1 und Artikel 62 Absatz 1 Buchstabe a der vorgeschlagenen Verordnung vorgesehen). Wie in seiner Stellungnahme vom 7. März 2012 unterstrichen, würden diese Befugnisse der Kommission die in Kapitel VI vorgesehene Unabhängigkeit der nationalen Aufsichtsbehörden untergraben, was nicht mit dem AEUV, der Charta der Grundrechte der Europäischen Union und dem Fallrecht des Gerichtshofs der Europäischen Union vereinbar wäre.

43. Unter den vorgeschlagenen Optionen bevorzugt der EDSB diejenigen, die im Entwurf des Albrecht-Berichts zu den Kapiteln VI und VII enthalten sind. Der Entwurf des Berichts lässt jedoch einige Fragen im Hinblick auf den Aufbau des Systems offen. Der EDSB ist der Ansicht, dass die Rolle des Europäischen Datenschutzausschusses im Kohärenzverfahren in Bezug auf Fragen überdacht werden muss wie beispielsweise, ob dieser verbindliche Entscheidungen erlässt oder nicht und falls ja, auf welche Weise. Dabei ist insbesondere auch zu berücksichtigen, dass Bedarf an einer einheitlichen Regelung in der EU besteht und dass natürlichen Personen und Organisationen die Möglichkeit eingeräumt werden

muss, Rechtsmittel einzulegen. Der Ausgangspunkt dieser Überlegungen sollte sein, dass die nationalen Aufsichtsbehörden in ihrem einzelstaatlichen Rechtssystem weiterhin primär zuständig und verantwortlich bleiben.

44. **Der EDSB empfiehlt die Zurückweisung der in der ITRE-Stellungnahme vorgeschlagenen Abänderungen**, welche das Kohärenzverfahren schwächen und mächtigen Lobbys eine wichtige Rolle einräumen würden. Der EDSB spricht sich auch gegen Abänderungen aus, die darauf abzielen, den für die Verarbeitung Verantwortlichen, den betroffenen Personen oder den „betroffenen Akteuren" die Möglichkeit einzuräumen, das Kohärenzverfahren auszulösen, da dies dazu führen würde, dass das System nicht zu verwirklichen wäre (siehe beispielsweise IMCO AM 195 oder ITRE AM 352). Natürliche Personen sollten stets in der Lage sein, Rechtsmittel vor ihren eigenen nationalen Gerichten einzulegen.

45. Abschließend vertritt der EDSB die Ansicht, dass der Europäische Datenschutzausschuss von einem angemessenen IT-Tool zur Unterstützung des Informationsaustausches zwischen Aufsichtsbehörden, wie dem Internal Market Information System IMI[13] profitieren könnte, und stellt fest, dass – sofern die Verwendung eines IT-Tools erwogen werden sollte – es erforderlich sein könnte, eine Rechtsgrundlage in die Verordnung aufzunehmen.

VIII. SANKTIONEN

46. Der EDSB erinnert daran, dass er in seiner Stellungnahme vom 7. März 2012 eine Stärkung des neuen Rechts von Organisationen und Verbänden befürwortet hat, die sich den Schutz der Rechte und Interessen betroffener Personen zum Ziel gesetzt haben, Beschwerde bei einer Aufsichtsbehörde oder Klage zu erheben (siehe Artikel 73 und 76 der vorgeschlagenen Verordnung). Aus diesem Grund ist er der Ansicht, dass **Abänderungen, die derartige Sammelklagen schwächen** (oder sogar ganz streichen, wie in LIBE AM 2777 ff.) **nicht unterstützt werden sollten.**

47. In der Stellungnahme rief der EDSB auch zu mehr Flexibilität bei der Anwendung von Sanktionen auf, die im Hinblick auf Verstöße gegen die Verordnung verhängt werden. Der Ermessensspielraum der Aufsichtsbehörden ist ein unerlässliches Element eines konsequenten und anpassbaren Vollstreckungssystems, insbesondere im Hinblick auf die verschiedenen Optionen, die den Aufsichtsbehörden zur Verfügung stünden, um bei Verstößen gegen die Verordnung Sanktionen zu verhängen, die *Abhilfe* schaffen (siehe Artikel 53 Absatz 1 Buchstabe a). Von diesem Standpunkt aus betrachtet, **begrüßt der EDSB Abänderungen, die den Aufsichtbehörden einen größeren Ermessensspielraum im Hinblick auf die Frage einräumen, ob sie eine Sanktion auferlegen oder nicht**, insbesondere, falls die festgestellte Verletzung nicht vorsätzlich erfolgt ist (z. B. Albrecht AM 318). Gleichzeitig ist er der Ansicht, dass die Aufnahme von Listen zusätzlicher „erschwerender" oder „abschwächender" Kriterien (wie in Albrecht AM 316-317, ITRE AM 371-372, IMCO AM 206-207) eingehender zu prüfen ist, um sicherzustellen, dass ein angemessenes Gleichgewicht gewahrt wird zwischen der

[13] Das IMI wurde förmlich durch die Verordnung (EU) Nr. 1024/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 über die Verwaltungszusammenarbeit mit Hilfe des Binnenmarkt-Informationssystems und zur Aufhebung der Entscheidung 2008/49/EG der Kommission eingeführt, ABl. L 316 vom 14.11.2012.

Rechtssicherheit einerseits und der Notwendigkeit für die Aufsichtsbehörden anderseits, ihre Befugnisse mit ausreichender Flexibilität auszuüben.

48. Abschließend begrüßt der EDSB die Versuche, für **Kohärenz** im Hinblick auf den Ansatz zur Verhängung von Sanktionen auf der Ebene der EU zu sorgen, zum Beispiel über den Europäischen Datenschutzausschuss (z. B. mittels Leitlinien und Informationsaustausch über die verhängten Sanktionen).

IX. VORLÄUFIGE FESTSTELLUNGEN ZUR RICHTLINIE[14]

1. Anwendungsbereich

49. Wie in Abschnitt II Punkt 1 Buchstabe a oben erläutert, begrüßt es der EDSB grundsätzlich, dass die vorgeschlagene Richtlinie auch für Organe und Einrichtungen der EU gilt (LIBE AM 270-272), obgleich er unterstreichen möchte, dass angesichts des spezifischen rechtlichen und institutionellen Rahmens, in dem diese tätig sind, weiterer Klärungsbedarf besteht, der in den derzeit vorliegenden Vorschlägen nicht angegangen wird.

2. Datenschutzgrundsätze

50. Der EDSB stellt fest, dass verschiedene Abänderungen darauf abzielen, die Frage der weiteren Verarbeitung zur „**nicht zweckentsprechenden Verwendung**" anzugehen. Der EDSB erinnert daran, dass jede Ausnahme vom Grundsatz der „zweckentsprechenden Verwendung" nur zu Zwecken zulässig ist, die klar und erschöpfend definiert sind und angemessenen Garantien unterliegen. In diesem Kontext stellt er fest, dass die LIBE-Abänderungen 66, 347 und 350 verschiedene positive Elemente enthalten, die als Grundlage für die weitere Entwicklung verwendet werden könnten. Wie oben erwähnt (siehe Abschnitt III.1) möchte der EDSB die Aufmerksamkeit auf die Stellungnahme der WP 29 zur Zweckbindung lenken, die in den nächsten Wochen angenommen werden wird. Diese Stellungnahme wird weitere Leitlinien und Kriterien für ein einheitliches Verständnis des Begriffs „zweckentsprechende Verwendung" enthalten.

51. Der EDSB begrüßt die Abänderungen, welche die Verpflichtung stärken, zwischen den verschiedenen Kategorien von betroffenen Personen und dem unterschiedlichen Grad der Richtigkeit und Verlässlichkeit der Daten zu unterscheiden (z. B. LIBE AM 60, 318-319). Diese Verpflichtungen – die spezifisch für den Strafverfolgungsbereich gelten – sind sowohl für betroffene Personen als auch für Strafverfolgungsbehörden von Bedeutung. Vergleichbare Verpflichtungen sind auch für die EU-Rechtsvorschriften im Bereich der polizeilichen Zusammenarbeit vorgesehen[15]. In diesem Kontext sind die LIBE-Abänderungen 314-317, welche die Verpflichtung zur Unterscheidung zwischen Kategorien von betroffenen Personen streichen, nicht annehmbar.

52. Der EDSB begrüßt die Abänderungen, welche eine Verpflichtung der Mitgliedstaaten vorsehen, spezifische Vorschriften bezüglich der Folgen der Kategorisierung von betroffenen Personen einzuführen (LIBE AM 330-331).

[14] Diese vorläufigen Feststellungen basieren auf den LIBE-Abänderungen.
[15] Siehe beispielsweise Artikel 14 Absatz 1 des Europol-Beschlusses.

Ebenso begrüßt er die Abänderung LIBE AM 351, in der spezifische Garantien für nicht verdächtige Personen eingeführt werden, die den Empfehlungen der WP 29 in deren Stellungnahme vom 26. Februar [16]entsprechen.

3. Informationsaustausch mit privaten Parteien

53. Der EDSB begrüßt die Absicht, den Informationsaustausch zwischen dem Strafverfolgungsbereich und privaten Parteien zu regeln, um so bis zu einem gewissen Maß die rechtliche Unsicherheit im Hinblick auf Situationen zu klären, in denen die Aktivitäten des privaten Sektors und des Strafverfolgungsbereichs miteinander interagieren (d. h. sofern Daten zu kommerziellen Zwecken erfasst werden und ein weiterer Zugriff zu Strafverfolgungszwecken erfolgt, aber auch sofern Informationen von einer Strafverfolgungsbehörde an private Parteien oder Behörden übermittelt werden, die keine Strafverfolgungsbehörden sind).

54. Was den **Zugriff von Strafverfolgungsbehörden auf Daten angeht, die anfänglich zu Zwecken verarbeitet wurden, die nicht mit der Strafverfolgung verbunden sind**, nimmt der EDSB erfreut zur Kenntnis, dass LIBE AM 58 und 310 spezifische Bedingungen und Garantien bezüglich des Zugangs zu diesen Daten einführen. Er ist jedoch der Ansicht, dass die Abänderung LIBE AM 310, die lediglich eine gültige Rechtsgrundlage vorsieht, die ausreichende Garantien für die betroffene Person bietet, zu weitgehend ist und die erforderlichen Garantien nicht enthält. Diese Abänderung allein sollte deshalb nicht angenommen werden.

55. Was die Datenübermittlung durch Strafverfolgungsbehörden an andere Parteien (d. h. Behörden, die keine Strafverfolgungsbehörden sind, und private Parteien) angeht, begrüßt der EDSB die Absicht, diese Frage anzugehen und spezifische Bedingungen für diese Übermittlung einzuführen (z. B. LIBE AM 162). Er möchte jedoch die Aufmerksamkeit insbesondere auf die Abänderungen lenken, die darauf abzielen, die Übermittlungen an Behörden, die keine Strafverfolgungsbehörden sind, und an private Parteien außerhalb der EU zu regeln (LIBE AM 589-590), da der vorgeschlagene Wortlaut dieser Abänderungen das Schutzniveau schwächt (siehe unten „Weitergabe von Daten an Dritte“).

4. Rollen und Verantwortlichkeiten des für die Verarbeitung Verantwortlichen

56. Der EDSB begrüßt Abänderungen, welche wesentliche Elemente des Grundsatzes der Rechenschaftspflicht einführen, die im Vorschlag der Kommission fehlen. Der EDSB begrüßt insbesondere die Verpflichtung des für die Verarbeitung Verantwortlichen, die Einhaltung der Bestimmungen *nachzuweisen* (z. B. LIBE AM 480), eine Datenschutzfolgenabschätzung durchzuführen (z. B. LIBE AM 27-28, 110, 113) und die Datenschutzbehörde vor der Verarbeitung personenbezogener Daten zu Rate zu ziehen (z. B. LIBE AM 541 bis 543). Er begrüßt auch verschiedene weitere Abänderungen, welche die Rolle und den Status des DSB stärken (z. B. LIBE AM 120-123, 570, 573, 575-576, 578).

[16] Stellungnahme 01/2013 vom 26. Februar 2013 mit weiteren Beiträgen zur Diskussion über den Vorschlag für eine 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.

5. Datenübermittlung an Drittländer

57. Der EDSB begrüßt die gestellte Anforderung, wonach der für die Verarbeitung Verantwortliche in einem Drittland oder einer internationalen Organisation eine für die Strafverfolgung zuständige Behörde sein sollte (LIBE AM 126, 584), wie in bestehenden Rechtsinstrumenten im Bereich der polizeilichen und justiziellen Zusammenarbeit vorgesehen. Außerdem begrüßt er im Wesentlichen die zusätzlichen Bedingungen, die von den LIBE-Abänderungen 126 und 591 vorgesehen sind.

58. Er ruft in Erinnerung, dass **jede Übermittlung an Behörden, die keine Strafverfolgungsbehörden sind, oder an private Parteien streng einschränkt sein und strengen Garantien unterliegen sollte**. Dies ist insbesondere dann wichtig, wenn diese Empfänger sich außerhalb der EU befinden. Wie oben bereits erwähnt, bieten die LIBE-Abänderungen 589 und 590, die eine derartige Übermittlung vorsehen, keine angemessenen Garantien. Außerdem werfen diese Abänderungen ernsthafte Bedenken auf, da ausgehend von ihrem aktuellen Wortlaut die Datenübermittlung an Behörden, die keine Strafverfolgungsbehörden sind, oder an private Parteien in Drittländern einfacher wäre als an Strafverfolgungsbehörden.

59. In seiner Stellungnahme vom 7. März 2012 kritisierte der EDSB die Tatsache, dass allein die Beurteilung durch den für die Verarbeitung Verantwortlichen als Rechtsgrundlage für Übermittlungen an ein Drittland ausreichend wäre und begrüßt folglich die Abänderungen, die vorschlagen, diese Möglichkeit zu annullieren (LIEBE AM 33, 602).

6. Befugnisse der Aufsichtsbehörden

60. In seiner Stellungnahme hat der EDSB unterstrichen, dass selbst wenn beschränkte Ausnahmen **im Hinblick auf Gerichte** gerechtfertigt sind, **die in ihrer gerichtlichen Eigenschaft tätig werden**, er keinen Grund dafür sieht, die Befugnisse der Aufsichtsbehörden außerhalb dieses spezifischen Kontextes einzuschränken. Er begrüßt deshalb die Abänderungen zur Angleichung der Befugnisse der Aufsichtsbehörden gegenüber Strafverfolgungsbehörden an die in der vorgeschlagenen Verordnung vorgesehenen Befugnisse (z. B. LIBE AM 142-645). Er begrüßt auch die LIBE-Abänderungen 645 und 649, da sie die Bedenken der WP 29 hinsichtlich der Notwendigkeit aufgreifen, i) sicherzustellen, dass alle beteiligten Aufsichtsbehörden Zugang zu denselben Informationen haben und ii) die zugänglichen Informationen zu identifizieren[17].

[17] Stellungnahme 01/2013 vom 26. Februar 2013 mit weiteren Beiträgen zur Diskussion über den Vorschlag für eine 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.

7. Spezifische Rechtsakte im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

61. In seiner Stellungnahme hat der EDSB bedauert, dass spezifische Rechtsakte im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen unberührt geblieben sind. Er hat unterstrichen, dass der Zweijahreszeitraum, auf den in Artikel 61 Absatz 2 der vorgeschlagenen Richtlinie verwiesen wird, für die Überprüfung dieser Rechtsakte durch die Kommission zu einem inakzeptabel langen Zeitraum führen würde, in dem das aktuelle, vielfach kritisierte Flickwerk bestehen bleibt. Aus diesem Grund ist die LIBE-Abänderung 671, welche die Pflicht zu einer derartigen Überprüfung streicht, inakzeptabel.

Brüssel, den 15. März 2013