



## **Stellungnahme des Europäischen Datenschutzbeauftragten**

**zum „Offene Daten-Paket“ der Europäischen Kommission mit einem Vorschlag für eine Richtlinie zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors, zu einer Mitteilung zum Thema „Offene Daten“ und dem Beschluss 2011/833/EU der Kommission über die Weiterverwendung von Kommissionsdokumenten**

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE -

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr<sup>1</sup>,

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr<sup>2</sup>, insbesondere auf Artikel 41 Absatz 2,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

### **1. EINLEITUNG**

#### **1.1. Hintergrund**

1. Am 12. Dezember 2011 nahm die Kommission einen Vorschlag für eine Richtlinie zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors („Vorschlag“) an.<sup>3</sup> Der Vorschlag ist Bestandteil des „Offene Daten-Pakets“, zu dem noch zwei weitere, am selben Tag angenommene Dokumente gehören: i) eine Mitteilung der Kommission mit dem Titel „Offene Daten: Ein Motor für Innovation, Wachstum und transparente Verwaltung“ („Mitteilung“)<sup>4</sup> und ii) ein

---

<sup>1</sup> ABl. L 281 vom 23.11.1995, S. 31.

<sup>2</sup> ABl. L 8 vom 12.1.2001, S. 1.

<sup>3</sup> KOM(2011) 877 endgültig.

<sup>4</sup> KOM(2011) 882 endgültig.

Beschluss der Kommission über die Weiterverwendung von Kommissionsdokumenten („Beschluss“)<sup>5</sup>.

2. Entgegen der Bestimmung in Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 wurde der EDSB nicht konsultiert. Dies ist in Anbetracht der von dieser Initiative möglicherweise betroffenen großen Menge personenbezogener Daten bedauerlich. Die vorliegende Stellungnahme stützt sich daher auf Artikel 41 Absatz 2 dieser Verordnung. Der EDSB empfiehlt, in die Präambel des angenommenen Instruments einen Verweis auf diese Stellungnahme aufzunehmen.

## **1.2. Ziele und Geltungsbereich des Vorschlags und des Beschlusses; Schwerpunkt der Stellungnahme des EDSB**

3. Ziel des Vorschlags ist es, den Wortlaut der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors („PSI-Richtlinie“) zu aktualisieren und zu ändern.
4. Ziel der PSI-Richtlinie ist es, die unionsweite Weiterverwendung von Informationen des öffentlichen Sektors dadurch zu erleichtern, dass die Grundvoraussetzungen für die Weiterverwendung geschaffen und Hindernisse beseitigt werden, die einer Weiterverwendung im Binnenmarkt entgegenstehen. Die PSI-Richtlinie enthält Regelungen in Bezug auf die Nichtdiskriminierung, die Gebührenerhebung, Ausschließlichkeitsvereinbarungen, die Transparenz und die Lizenzvergabe sowie praktische Instrumente, die das Auffinden und die Weiterverwendung öffentlicher Dokumente erleichtern.<sup>6</sup>
5. Eines der zentralen neuartigen politischen Ziele des Vorschlags besteht, wie in Abschnitt 5.1 der Mitteilung beschrieben, darin, den Grundsatz einzuführen, dass „alle öffentlichen Informationen, die nicht eindeutig unter eine der Ausnahmen fallen, für gewerbliche und nichtgewerbliche Zwecke weiterverwendet werden dürfen“.<sup>7</sup> So wird insbesondere in der vorgeschlagenen Änderung von Artikel 3 Absatz 1 der PSI-Richtlinie von den Mitgliedstaaten verlangt, sicherzustellen, dass „Dokumente“, die im Besitz öffentlicher Stellen der Mitgliedstaaten sind, „für gewerbliche und nichtgewerbliche Zwecke weiterverwendet werden können“.
6. Weitere relevante neue Bestimmungen des Vorschlags betreffen, vorbehaltlich einiger Ausnahmen, die Beschränkung der Beträge, die von öffentlichen Stellen für die Weiterverwendung von Dokumenten erhoben werden, auf „die durch die Vervielfältigung und Weiterverbreitung verursachten Zusatzkosten“ (überarbeiteter Artikel 6 Absatz 1). Darüber hinaus erweitert der Vorschlag den Geltungsbereich der PSI-Richtlinie auf Bibliotheken, Archive, Museen und Universitätsbibliotheken.
7. Ziel des Beschlusses ist es, Bedingungen festzulegen, unter denen die Kommission ihre eigenen Dokumente weiterverwenden darf.

---

<sup>5</sup> 2011/833/EU.

<sup>6</sup> Siehe die Begründung des Vorschlags, Abschnitt 1.

<sup>7</sup> Siehe ferner Abschnitt 3.2 Absatz 6 der Begründung des Vorschlags, dem zufolge Maßnahmen auf Unionsebene notwendig sind, um „dafür [zu] sorgen, dass [...] die Weiterverwendung von wertvollen Kerndaten des öffentlichen Sektors in allen Mitgliedstaaten erlaubt wird“, sowie Abschnitt 5, Kapitel „Änderungen der Rechtsvorschriften“, Punkt iii) der Zusammenfassung der Folgenabschätzung, wo eine „Änderung des allgemeinen Grundsatzes“ gefordert wird, „um verfügbare Dokumente auch weiterverwendbar zu machen“.

8. Im Mittelpunkt der Abschnitte 2 und 3 der vorliegenden Stellungnahme steht der Vorschlag, während sich Abschnitt 4 kurz mit dem Beschluss befasst. Abschnitt 2 bietet einen allgemeinen Überblick über die datenschutzrechtlichen Bedenken im Zusammenhang mit offenen Daten, geht auf die Herausforderungen ein und stellt Betrachtungen an, die als wichtige Bezugspunkte dienen und weitgehend den Ansatz bestimmen, den der EDSB in seinen spezifischeren Empfehlungen in Abschnitt 3 verfolgt.

## **2. ALLGEMEINE ANMERKUNGEN**

### **2.1. Anwendung der Datenschutzvorschriften**

9. Einleitend weist der EDSB darauf hin, dass es zwar große Mengen von Informationen des öffentlichen Sektors gibt, die keine personenbezogenen Daten enthalten, dass öffentliche Stellen aber auch über große Mengen personenbezogener Daten unterschiedlicher Art und Schutzwürdigkeit verfügen. Als Beispiele seien genannt: Angaben über Geschäftsführer und andere Vertreter von in einem Handelsregister eingetragenen Unternehmen, Angaben zu Gehältern von Beamten oder Ausgaben von Parlamentsmitgliedern sowie die Krankenakten von Patienten eines nationalen Gesundheitsdienstes.
10. In diesem Zusammenhang sei darauf hingewiesen, dass alle Informationen über eine bestimmte oder bestimmbare natürliche Person, seien sie öffentlich verfügbar oder nicht, personenbezogene Daten sind. Außerdem bedeutet allein die Tatsache, dass derartige Daten öffentlich verfügbar gemacht wurden, noch keine Ausnahme von den Datenschutzvorschriften. Die Weiterverwendung personenbezogener Daten, die vom öffentlichen Sektor der Öffentlichkeit zur Verfügung gestellt wurden, unterliegt daher grundsätzlich weiterhin den einschlägigen Datenschutzvorschriften.<sup>8</sup>
11. Wie näher in Abschnitt 3.1 dargestellt, geht aus der vorgeschlagenen PSI-Richtlinie nicht klar hervor, ob sie auch auf personenbezogene Daten Anwendung findet, und wenn ja, unter welchen Bedingungen.

### **2.2. Wichtigste datenschutzrechtliche Bedenken**

12. Würden grundsätzlich alle Informationen des öffentlichen Sektors weiterverwendet, dürften diese Informationen deutlich leichter zugänglich sein. Damit ergäben sich möglicherweise Vorteile wie mehr Transparenz und innovative Weiterverwendung von Informationen des öffentlichen Sektors, einschließlich einiger Kategorien personenbezogener Daten.
13. Ein verstärkter Zugang zu Informationen kann aber auch das Risiko des Missbrauchs personenbezogener Daten steigern. Diese Risiken bestehen selbst dann, wenn die betreffenden personenbezogenen Daten gemäß der „Zugangsregelung“ des jeweiligen Mitgliedstaats der Öffentlichkeit bereits zugänglich gemacht wurden (oder ihr zugänglich gemacht werden können). Falls nicht angemessene Garantien angewandt und konsequent und wirksam durchgesetzt werden, kann die zur Weiterverwendung

---

<sup>8</sup> Siehe das Urteil des Europäischen Gerichtshofes vom 16. Dezember 2008 in der Rechtssache C-73/07 *Tietosuoja- ja valtuutettu vs Satakunnan Markkinapörssi Oy en Satamedia Oy*, Randnrn. 38-49. Siehe ferner Absatz 3 Abschnitt II.2 der Stellungnahme 7/2003 der Artikel 29-Datenschutzgruppe, vollständig in nachstehender Fußnote 11 zitiert.

bereitgestellte Information auf ungesetzliche Weise (überall in Europa und darüber hinaus) „geerntet“<sup>9</sup>, mit anderen Informationen kombiniert, verkauft und schließlich zu Zwecken verwendet werden kann, die i) ursprünglich nicht vorgesehen waren, ii) möglicherweise nicht verhältnismäßig sind und für die es iii) keine angemessene Rechtsgrundlage gibt. Zu den Risiken für den Schutz der Privatsphäre gehören auch kriminelle Aktivitäten wie Identitätsdiebstahl.

14. Derartige Risiken sind nicht völlig neuartig und bestehen für viele Großprojekte, bei denen große Mengen personenbezogener Daten, die zuvor in Papierform bei örtlichen Behörden aufbewahrt wurden, nun in digitaler Form im Internet der Öffentlichkeit zugänglich gemacht werden.<sup>10</sup>
15. Offene Daten-Projekte bedeuten allerdings eine völlig neue Stufe der Zugänglichkeit von Informationen. Bei vielen „Offene Daten“-Projekten werden nämlich i) ganze Datenbanken ii) in standardisiertem elektronischem Format und dies iii) ohne jegliches "Screening" allen Personen, die dies beantragen, iv) kostenlos und v) zu gewerblichen oder nichtgewerblichen Zwecken mit einer offenen Lizenz verfügbar gemacht. Diese neue Form der Zugänglichkeit ist der Hauptzweck offener Daten, doch ist sie nicht ganz ohne Risiken, wenn sie wahllos und ohne angemessene Garantien angewandt wird. Ein Beispiel: Ein herkömmliches e-Government-Portal, das der Öffentlichkeit Zugriff auf bestimmte personenbezogene Daten in einem Handelregister bietet, kann es, bei ordnungsgemäßer Konfiguration und mit angemessenen Sicherheitsvorkehrungen, für Dritte äußerst schwierig machen, den Inhalt der gesamten Datenbank zu „ernten“ (und damit in der Folge zu verwenden). Wird die gesamte Datenbank einfach allen interessierten Kreisen zur Weiterverwendung geöffnet, wachsen die Zugänglichkeit und die ihr innewohnenden Risiken exponentiell.

### **2.3. Weiterverwendung von Informationen des öffentlichen Sektors nach dem bestehenden Datenschutzrahmen**

16. Um datenschutzrechtlichen Bedenken Rechnung zu tragen, verweist die PSI-Richtlinie auf den allgemeinen Datenschutzrahmen.
  - Gemäß Erwägungsgrund 21 sollte die PSI-Richtlinie „unter uneingeschränkter Beachtung der Grundsätze des Schutzes personenbezogener Daten [...] durchgeführt und angewandt werden“, und
  - Artikel 1 Absatz 4 besagt, dass die PSI-Richtlinie „keinerlei Auswirkungen auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ hat.
17. Allerdings enthalten weder die derzeitige PSI-Richtlinie noch der Vorschlag irgendwelche spezifischen Datenschutzbestimmungen, in denen darauf eingegangen wird, dass sie die Weiterverwendung großer Mengen von Informationen des öffentlichen Sektors zulassen und erhebliche Auswirkungen auf den Datenschutz haben können.

---

<sup>9</sup> Zu internationalen Übermittlungen und der Weiterverwendung von PSI durch Organisationen in Drittländern siehe nachstehenden Abschnitt 3.4.

<sup>10</sup> Siehe beispielsweise Abschnitt III.1 der Stellungnahme des EDSB zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinien 89/666/EWG, 2005/56/EG und 2009/101/EG in Bezug auf die Verknüpfung von Zentral-, Handels- und Gesellschaftsregistern, ABl. C 220 vom 26.7.2011, S. 1).

18. In diesem Zusammenhang bot die Artikel 29-Datenschutzgruppe (WP 29) 2003 Hilfestellung in Bezug auf die Anwendung des derzeitigen Datenschutzrahmens auf die Weiterverwendung von Informationen des öffentlichen Sektors, sofern diese personenbezogene Daten enthalten.<sup>11</sup> Die Stellungnahme der WP 29 hatte den Grundsatz der Zweckbindung<sup>12</sup> in den Mittelpunkt gestellt, befasste sich aber auch mit anderen Fragen wie der Rechtmäßigkeit (Rechtsgrundlage) der Weitergabe von Informationen des öffentlichen Sektors an die Öffentlichkeit und ihrer Weiterverwendung, dem besonderen Schutz sensibler Daten, Übermittlungen an Drittländer, Datenqualität und Rechten betroffener Personen.
19. Die Stellungnahme der WP 29 zeigt, dass die Anwendung des geltenden Datenschutzrahmens auf die Weiterverwendung von Informationen des öffentlichen Sektors eine Reihe von Problemen aufwirft.
20. So ist es insbesondere nicht einfach, den Grundsatz der Zweckbindung bei der Weiterverwendung von PSI wirksam umzusetzen. Zum einen liegen der Grundgedanke und die treibende Kraft für Innovation hinter dem Begriff „offene Daten“ und der Weiterverwendung von Informationen des öffentlichen Sektors darin, dass die Informationen für die Weiterverwendung in innovativen neuen Projekten und Dienstleistungen und damit für Zwecke zur Verfügung stehen, die zuvor nicht festgelegt wurden und nicht eindeutig vorhersehbar sind. Zum anderen gehört die Zweckbindung zu den Kerngrundsätzen des Datenschutzes und erfordert, dass personenbezogene Daten, die für einen konkreten Zweck erhoben wurden, später nicht für einen anderen, mit dem ursprünglichen Zweck nicht zu vereinbarenden Zweck verwendet werden, es sei denn, bestimmte Zusatzbedingungen sind erfüllt.<sup>13</sup> Diese beiden Anliegen (offene Daten und Datenschutz) sind nicht leicht miteinander zu vereinbaren.
21. Die Herausforderung liegt darin, vorab zu bestimmen, welche personenbezogenen Daten der Öffentlichkeit zugänglich gemacht werden könnten, und mit welchen angemessenen Datenschutzgarantien Rechtssicherheit gewährleistet werden kann, und gleichzeitig Innovation und die Weiterverwendung für (rechtmäßige) Zwecke zuzulassen.
22. Ein weiterer Kerngrundsatz der Richtlinie 95/46/EG ist die Verhältnismäßigkeit<sup>14</sup>. Personenbezogene Daten werden der Öffentlichkeit mit verschiedenen Methoden, Modalitäten und mit unterschiedlicher Granularität zur Verfügung gestellt. Einige von ihnen dringen unter Umständen stärker in die Privatsphäre ein als andere und bergen größere Risiken. Folglich dürften einige von ihnen als verhältnismäßig gelten, andere

---

<sup>11</sup> Siehe Stellungnahme 7/2003 zur Weiterverwendung von Informationen des öffentlichen Sektors und Schutz personenbezogener Daten – Interessenabwägung – der Artikel 29-Datenschutzgruppe, angenommen am 12. Dezember 2003 (WP 83). Siehe zwei weitere thematisch verwandte Stellungnahmen der WP 29: Stellungnahme 3/1999 über Informationen des öffentlichen Sektors und den Schutz personenbezogener Daten, angenommen am 3. Mai 1999 (WP 20) sowie Stellungnahme 5/2001 zu einem Sonderbericht des Europäischen Bürgerbeauftragten, angenommen am 17. Mai 2001.

<sup>12</sup> Siehe Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG.

<sup>13</sup> Dieser Grundsatz gilt auch für öffentlich verfügbare personenbezogene Daten. Allein die Tatsache, dass personenbezogene Daten für einen konkreten Zweck öffentlich verfügbar sind, bedeutet nicht zwangsläufig, dass diese personenbezogenen Daten auch für die Weiterverwendung zu anderen Zwecken zur Verfügung stehen.

<sup>14</sup> Siehe Artikel 6 Absatz 1 Buchstabe c der Richtlinie 95/46/EG.

hingegen nicht.<sup>15</sup> Eine weitere große Herausforderung liegt also darin, die Verhältnismäßigkeit zu wahren und dabei genügend Spielraum zu lassen.

23. In einem ähnlichen Zusammenhang, nämlich mit Blick auf ein ausgewogenes Verhältnis zwischen dem Recht auf Schutz personenbezogener Daten und dem Recht auf den Zugang der Öffentlichkeit zu Dokumenten, hat der EDSB den Organen und Einrichtungen der EU einen „proaktiven Ansatz“ in dieser Frage empfohlen. Ein solcher Ansatz würde erfordern, dass der Geltungsbereich einer Offenlegung personenbezogener Daten für die Öffentlichkeit proaktiv und möglichst früh analysiert wird und dass betroffene Personen entsprechend in Kenntnis gesetzt werden, damit sie ihre Rechte ausüben können.<sup>16</sup> Mit diesem Ansatz lassen sich fallweise angemessene Lösungen finden, und er dürfte auch für eine mögliche Weiterverwendung von Informationen des öffentlichen Sektors, die personenbezogene Daten enthalten, von Belang sein.

#### **2.4. Der Vorschlag sollte konkreter auf den Datenschutz eingehen**

24. Zwar bietet die Richtlinie 95/46/EG einen soliden rechtlichen Rahmen und enthalten die Stellungnahmen der Artikel 2-Datenschutzgruppe wichtige Klarstellungen, doch sollten darüber hinaus auch einige Bestimmungen der PSI-Richtlinie klarer formuliert und näher ausgeführt werden, um so ein höheres und kohärenteres Datenschutzniveau überall in der Europäischen Union sowie mehr Rechtssicherheit für betroffene Personen zu erreichen.

25. Beim derzeitigen Stand der Harmonisierung des Rechts in Europa bestehen erhebliche Unterschiede zwischen den einzelstaatlichen Vorschriften und Vorgehensweisen im Hinblick auf die Weiterverwendung von Informationen des öffentlichen Sektors. So weichen insbesondere die Haltung zur Transparenz und als Folge dessen auch die Rechtsvorschriften der Mitgliedstaaten über den Zugang zu Dokumenten voneinander ab. Auch behandeln die nationalen Datenschutzgesetze zur Umsetzung der Richtlinie 95/46/EG dieses Thema nicht immer in ähnlicher Weise.

26. Trotz dieser Unterschiede müssen die betroffenen Personen darauf vertrauen können, dass ihre Daten ungeachtet der Übermittlung in einen anderen Mitgliedstaat zum Zweck der Weiterverwendung konsequent geschützt werden.

27. Unnötige Komplexität und Fragmentierung sollten ferner nicht nur vermieden werden, um betroffenen Personen angemessenen Schutz gewährleisten zu können, sondern auch, um den freien Datenverkehr zu ermöglichen, ein weiteres zentrales Ziel der Richtlinie 95/46/EG.

---

<sup>15</sup> Siehe beispielsweise das Urteil des EuGH vom 9. November 2010, verbundene Rechtssachen C-92/09 und C-93/09 (*Schecke und Eifert*); insbesondere Randnrn. 81, 85 und 86. In dieser Rechtssache betonte der EuGH, dass sich Ausnahmen und Beschränkungen in Bezug auf den Schutz personenbezogener Daten auf das absolut Notwendige beschränken müssen. Der EuGH vertrat insbesondere die Auffassung, die europäischen Organe sollten andere Modalitäten der Veröffentlichung erkunden, die im Einklang mit dem Zweck einer solchen Veröffentlichung stehen, zugleich aber auch in das Recht der betroffenen Personen auf Achtung ihres Privatlebens und auf Schutz ihrer personenbezogenen Daten weniger stark eingreifen.

<sup>16</sup> Siehe das Papier des EDSB „Zugang der Öffentlichkeit zu Dokumenten mit personenbezogenen Daten nach dem Urteil in der Rechtssache *Bavarian Lager*“ vom 24. März 2011, abrufbar auf der Website des EDSB (<http://www.edps.europa.eu>), vor allem Kapitel III auf S. 7ff.

28. Die vom thematischen Netzwerk LAPSI<sup>17</sup> im Dezember 2011 ausgearbeiteten „Draft Policy Recommendations on Privacy“ illustrieren deutlich, wie es bei der Umsetzung der PSI-Richtlinie in den Mitgliedstaaten im Hinblick auf den Datenschutz zu sehr unbefriedigenden und unnötigen Unterschieden gekommen ist.
29. In Anbetracht der Tatsache, dass der Rechtsrahmen für den Datenschutz derzeit überarbeitet wird<sup>18</sup>, ist der EDSB ferner der Auffassung, dass es gegebenenfalls angebracht wäre, neue Konzepte wie „eingebauten Datenschutz“ und Verantwortung (accountability) zu berücksichtigen und praktische Instrumente wie Datenschutzfolgenabschätzungen im Vorschlag ausdrücklich zu erwähnen.<sup>19</sup>
30. Aus diesen Gründen empfiehlt der EDSB, dass der Vorschlag nicht nur die „Grundsätze des Schutzes personenbezogener Daten“ (siehe Erwägungsgrund 21) erwähnen, sondern darüber hinaus eindeutiger festlegen sollte, unter welchen Bedingungen und vorbehaltlich welcher Garantien, wie in Abschnitt 3 näher ausgeführt, die Bereitstellung von Informationen, die personenbezogene Daten enthalten, zur Weiterverwendung beantragt werden kann.

### 3. SPEZIFISCHE EMPFEHLUNGEN

#### 3.1. Die Anwendbarkeit des Grundsatzes der Weiterverwendung auf personenbezogene Daten sollte klargestellt und von weiteren Bedingungen abhängig gemacht werden

*Einschlägige Bestimmungen: Artikel 1 Absatz 2 Buchstabe c und Artikel 1 Absatz 3*

31. So wird insbesondere in der vorgeschlagenen Änderung von Artikel 3 Absatz 1 der PSI-Richtlinie (in Verbindung mit Artikel 1 Absatz 1)<sup>20</sup> von den Mitgliedstaaten verlangt, sicherzustellen, dass „Dokumente“, die im Besitz öffentlicher Stellen der Mitgliedstaaten sind, „für gewerbliche und nichtgewerbliche Zwecke weiterverwendet werden können.“
32. Weder die derzeitige PSI-Richtlinie noch der Vorschlag enthalten irgendwelche spezifischen Ausnahmen für personenbezogene Daten. Gemäß Artikel 1 Absatz 2 Buchstabe c gilt die PSI-Richtlinie nicht für „Dokumente, die nach den Zugangsregelungen der Mitgliedstaaten nicht zugänglich sind, einschließlich aus Gründen des Schutzes der nationalen Sicherheit (d. h. der Staatssicherheit), der Verteidigung oder der öffentlichen Sicherheit, [und] der statistischen oder gewerblichen Geheimhaltung“.

---

<sup>17</sup> LAPSI ist ein, von der Kommission finanziertes, europäisches thematisches Netzwerk, das sich mit den rechtlichen Aspekten von Informationen des öffentlichen Sektors (Legal Aspects of Public Sector Information) befasst; siehe <http://www.lapsi-project.eu/>. Die letzte Fassung der „Draft Policy Recommendations“ ist abrufbar unter [http://www.lapsi-project.eu/wiki/index.php/Policy\\_recommendation\\_on\\_privacy](http://www.lapsi-project.eu/wiki/index.php/Policy_recommendation_on_privacy).

<sup>18</sup> Siehe den Vorschlag der Kommission für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (COM(2012) 11 final). Siehe auch die Stellungnahme des EDSB zum Datenschutzreformpaket vom 7. März 2012, abrufbar unter [http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Reform\\_package.jsessionid=46ACCFDB9005EB950DF9C7D58BDE5377](http://www.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package.jsessionid=46ACCFDB9005EB950DF9C7D58BDE5377).

<sup>19</sup> Siehe z. B. die Empfehlung der Kommission vom 9. März 2012 zu Vorbereitungen für die Einführung intelligenter Messsysteme C(2012) 1342 endgültig.

<sup>20</sup> Falls nicht anders angegeben, wird auf die überarbeiteten Artikel der PSI-Richtlinie in der vorgeschlagenen Fassung verwiesen.

33. Artikel 1 Absatz 3 bestimmt weiter: Die PSI-Richtlinie „stützt sich auf die geltenden Zugangsregelungen der Mitgliedstaaten“ und „gilt nicht in den Fällen, in denen Bürger oder Unternehmen im Rahmen der Zugangsregelung ein besonderes Interesse am Zugang zu den Dokumenten nachweisen müssen“.
34. Diese Bestimmungen bedeuten, dass Dokumente, die personenbezogene Daten enthalten, nur unter die PSI-Richtlinie fallen, wenn diese Dokumente nach Maßgabe der „Zugangsregelungen der Mitgliedstaaten“ der Öffentlichkeit bereits zur Verfügung stehen oder verfügbar gemacht werden können.

*Artikel 1 Absatz 2 Buchstabe c sollte als Grund für die Verweigerung des Zugangs ausdrücklich den Schutz der Privatsphäre und den Schutz personenbezogener Daten erwähnen*

35. Artikel 1 Absatz 2 Buchstabe c gewährt den Mitgliedstaaten völlige Freiheit bei der Gestaltung ihrer „Zugangsregelung“ und enthält nur einige Beispiele für Gründe, aus denen ein Dokument „nicht zugänglich“ sein kann. In dieser Beispielreihe werden der Schutz der Privatsphäre und der Datenschutz derzeit nicht aufgeführt.
36. Im Sinne der Klarheit und der Stimmigkeit mit den allgemeinen Vorschriften über den Zugang der Öffentlichkeit zu Dokumenten empfiehlt der EDSB, Artikel 1 Absatz 2 Buchstabe c zu ändern und den Begriff „Schutz der Privatsphäre und personenbezogener Daten“ konkret bei den Beispielen für mögliche Gründe zu erwähnen, aus denen der Zugang verweigert werden kann.

*Beurteilung von Risiken für den Datenschutz und Garantien, mit denen sich solche Risiken mindern lassen*

37. Wie bereits in Abschnitt 2.2 gezeigt, bedeuten Offene Daten-Projekte eine neue Stufe des Zugangs zu Informationen und können erhebliche zusätzliche Risiken für den Schutz personenbezogener Daten beinhalten.
38. Diesbezüglich empfiehlt der EDSB, dass sich der Vorschlag zumindest ganz allgemein mit der Frage beschäftigt, wie die Weiterverwendung von Informationen des öffentlichen Sektors, die personenbezogene Daten enthalten, im Einklang mit den Datenschutzvorschriften erfolgen kann.
39. Es ist von entscheidender Bedeutung, dass öffentliche Stellen einen proaktiven Ansatz verfolgen<sup>21</sup>, wenn sie personenbezogene Daten für eine Weiterverwendung bereitstellen. Bei einem proaktiven Ansatz könnten die Daten der Öffentlichkeit ausdrücklich zur Weiterverwendung zugänglich gemacht werden, allerdings vorbehaltlich konkreter Bedingungen und Garantien im Einklang mit den Datenschutzvorschriften.
40. Zu diesem Zweck empfiehlt der EDSB, im Vorschlag vorzusehen, dass eine öffentliche Stelle, die personenbezogene Daten zur Weiterverwendung zur Verfügung stellt, vor ihrer Entscheidung der Frage nachgeht, ob die betroffenen personenbezogenen Daten überhaupt zur Weiterverwendung zur Verfügung gestellt werden dürfen. In dieser Beurteilung sollte auch festgelegt werden, unter welchen Bedingungen und vorbehaltlich welcher konkreten Datenschutzgarantien eine

---

<sup>21</sup> Siehe hierzu auch das in Fußnote 16 erwähnte Papier des EDSB.



Weiterverwendung zulässig ist. Eine solche Beurteilung wäre mit der in dem Vorschlag für eine allgemeine Datenschutzverordnung vorgesehenen Datenschutzfolgenabschätzung vergleichbar<sup>22</sup>. Der EDSB empfiehlt, die wichtigsten Elemente der Beurteilung in die vorgeschlagene Richtlinie aufzunehmen.

41. Die Beurteilung muss gewährleisten, dass nach nationalem Recht eine angemessene Rechtsgrundlage für die Übermittlung und Weiterverwendung der Daten besteht, dass eine Weiterverwendung nur zu einem vorschriftsgemäßen Zweck möglich ist, und dass Antragsteller alle anderen Bestimmungen des anzuwendenden Datenschutzrechts einhalten. Es können dort ferner zusätzliche Garantien angegeben werden. So kann beispielsweise die vollständige oder teilweise Anonymisierung der Daten vor ihrer Weiterverwendung verlangt und ein Verbot der erneuten Bestimmung betroffener Personen ausgesprochen werden (siehe nachstehende Punkte 45 und 46 sowie 56).
42. Gegebenenfalls kann von Antragstellern auch gefordert werden, in ihren Lizenzen bestimmten zusätzlichen Bedingungen zu entsprechen oder sogar selber eine Datenschutzfolgenabschätzung durchzuführen (siehe nachstehenden Punkt 53). In manchen Fällen kann die öffentliche Stelle auch die Zahl der zu vergebenden Lizenzen begrenzen und Lizenzen nur an Antragsteller vergeben, die bestimmten datenschutzrechtlichen Kriterien entsprechen (siehe nachstehenden Punkt 52).

### 3.2. Anonymisierung

*Auch teilweise anonymisierte und/oder aggregierte Daten können personenbezogene Daten enthalten*

43. Es sei darauf hingewiesen, dass die Daten so lange als „personenbezogene Daten“ gelten und damit den Datenschutzvorschriften unterliegen, wie natürliche Personen entweder unmittelbar oder mittelbar bestimmt werden können. Die Tatsache, dass einige „Anonymisierungstechniken“ angewandt wurden, heißt noch nicht, dass die Daten zwangsläufig als „anonymisiert“ im Sinne von Erwägungsgrund 26 der Richtlinie 95/46/EG gelten können.<sup>23</sup> Ein Datensatz kann personenbezogene Daten enthalten und möglicherweise zur Bestimmung einer natürlichen Person führen, auch wenn direkte Kennzeichen entfernt und mehrere zusätzliche Anonymisierungstechniken angewandt wurden.<sup>24</sup>
44. Eine vollständige Anonymisierung lässt sich nicht immer erreichen und wird aufgrund der Fortschritte der modernen Computertechnologie und von stets und überall verfügbaren Informationen immer schwieriger. Falls jedoch eine vollständige Anonymisierung nicht umfassend gewährleistet werden kann, gelten weiterhin Anforderungen des Datenschutzes; so muss beispielsweise eine angemessene Rechtsgrundlage für die Übermittlung und Weiterverwendung gegeben sein und es

---

<sup>22</sup> Zu Datenschutzfolgenabschätzungen siehe Artikel 33 des Vorschlags der Kommission für einen allgemeinen Datenschutzrahmen sowie die Punkte 200 bis 205 der in Fußnote 18 zitierten Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket.

<sup>23</sup> Erwägungsgrund 26, siehe vor allem die Passage: „Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem für die Verarbeitung Verantwortlichen oder einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen“.

<sup>24</sup> Siehe die Stellungnahme der Artikel 29-Datenschutzgruppe zum Begriff „personenbezogene Daten“ (WP 136), S. 15 bis 20. Siehe ferner das Urteil des House of Lords (Vereinigtes Königreich) vom 9. Juli 2008 in der Rechtssache *CSA v. SIC* sowie die einschlägigen Passagen in einer Reihe von Stellungnahmen des EDSB, beispielsweise Abschnitt 3.1 der Stellungnahme des EDSB vom 3. September 2010 zur Vorabkontrolle des Europäischen Überwachungssystems („TESSy“).

gelten der Grundsatz der Zweckbindung und der besondere Schutz für sensible Daten (wie gesundheitsbezogene Daten). Wann immer Daten nicht vollständig anonymisiert sind, muss die Einhaltung der Datenschutzvorschriften gewährleistet sein.

*Es ist ein angemessenes Maß an Anonymisierung zu gewährleisten*

45. Für diese Fälle empfiehlt der EDSB, im Vorschlag deutlich zum Ausdruck zu bringen, dass die öffentliche Stelle dafür zu sorgen hat, dass die betreffenden personenbezogenen Daten anonymisiert wurden und für eine Weiterverwendung nur in dieser anonymisierten Form zur Verfügung gestellt werden, es sei denn, die gemäß den vorstehenden Punkten 37 bis 42 vorgenommene Beurteilung ergibt in voller Übereinstimmung mit den geltenden Datenschutzvorschriften, dass die personenbezogenen Daten so bereitgestellt werden dürfen, dass die betroffenen Personen bestimmt werden können (z. B. Namen von Geschäftsführern in einem Handelsregister).
46. Aus der gemäß den Punkten 37 bis 42 durchgeführten Beurteilung sollte ferner hervorgehen, ob die Datenschutzvorschriften eine Bereitstellung der Daten zur Weiterverwendung auch nach einer nur teilweisen Anonymisierung zulassen und wenn ja, welcher Grad an Anonymisierung erforderlich ist, um das Risiko einer erneuten Bestimmung und des Missbrauchs der personenbezogenen Daten möglichst klein zu halten. Grundsätzlich sollte die Anonymisierung im erforderlichen Ausmaß erfolgen, wobei auf der einen Seite den Zwecken der Verarbeitung und auf der anderen Seite der Art der Daten und den potenziellen Folgen für die natürlichen Personen in dem Fall Rechnung getragen werden sollte, dass sie erneut bestimmt werden.<sup>25</sup>
47. Für den Fall, dass die Beurteilung ergibt, dass die personenbezogenen Daten nach einer teilweisen Anonymisierung für eine Weiterverwendung nicht zur Verfügung gestellt werden können und dass eine vollständige Anonymisierung nicht machbar ist, hält der EDSB fest, dass Informationen des öffentlichen Sektors, die personenbezogene Daten enthalten, nicht zwangsläufig und immer der Öffentlichkeit für eine Weiterverwendung zur Verfügung gestellt werden müssen. So können Daten beispielsweise zur Weiterverwendung nur einigen Lizenzinhabern überlassen werden, die anhand spezifischer Kriterien ausgewählt wurden.
48. So können beispielsweise (wenn alle anderen Datenschutzanforderungen erfüllt sind) feinkörnige Mikrodaten<sup>26</sup>, nach einer gewissen Anonymisierung, qualifizierten

---

<sup>25</sup> Ein Beispiel für aggregierte Daten, die vorbehaltlich bestimmter Garantien für eine Weiterverwendung zur Verfügung gestellt wurden, könnten die Straftatenkarten des Vereinigten Königreichs sein. Hier haben die Schöpfer des Datensatzes für die Weiterverwendung von Informationen nicht nur persönliche Kennzeichen (wie die Namen der Täter und Opfer begangener Straftaten) gelöscht, bevor sie die Daten zur Weiterverwendung bereitstellten, sondern sie haben die Daten auch so weit aggregiert, dass das Risiko einer erneuten Bestimmung und des Missbrauchs der Daten minimiert werden konnte. Dies war das Ergebnis einer Güterabwägung, bei der die Risiken möglichst klein gehalten werden sollten, gleichzeitig aber denjenigen, die etwas über die Kriminalitätsrate in einer bestimmten Gegend erfahren wollten, der gewünschte Detailgrad geliefert werden konnte.

<sup>26</sup> Mikrodaten sind „Datensätze, die Informationen zu einzelnen Befragten oder Unternehmen enthalten. Mit anderen Worten: Mikrodaten sind die bei Erhebungen gesammelten Grundinformationen...“ (Quelle: Eurostat, unter

[http://epp.eurostat.ec.europa.eu/portal/page/portal/research\\_methodology/statistical\\_confidentiality/confidential\\_data/introduction#microdata](http://epp.eurostat.ec.europa.eu/portal/page/portal/research_methodology/statistical_confidentiality/confidential_data/introduction#microdata)).

Siehe auch die Definition in Wikipedia (englische Fassung): [http://en.wikipedia.org/wiki/Microdata\\_\(statistics\)](http://en.wikipedia.org/wiki/Microdata_(statistics)): 'In the study of survey and census data, microdata is information at the level of individual respondents. For instance, a national census might collect age, home address, educational level, employment status, and many

Forschern, die sich einem strengen "Screening" unterzogen und zur Einhaltung strenger Lizenzbedingungen und zu strikter Vertraulichkeit verpflichtet haben, zu wissenschaftlichen Zwecken zur Verfügung gestellt werden.<sup>27</sup>

### 3.3. Lizenzen

*Einschlägige Bestimmung: Artikel 8*

49. Der vorgeschlagene Artikel 8 Absatz 1 lautet: „Öffentliche Stellen können die Weiterverwendung ohne Bedingungen gestatten oder aber Bedingungen, wie z. B. die Angabe der Quelle, in einer Lizenz festlegen. Diese Bedingungen dürfen die Möglichkeiten der Weiterverwendung nicht unnötig einschränken und nicht der Behinderung des Wettbewerbs dienen.“

*Datenschutzklausel*

50. Der EDSB empfiehlt, in Artikel 8 des Vorschlags eindeutig zu fordern, dass bei jeglicher Bereitstellung zur Weiterverwendung von Informationen des öffentlichen Sektors die personenbezogene Daten enthalten, die Lizenz eine spezifische Datenschutzklausel enthalten sollte.

51. Im Hinblick auf den Inhalt dieser Klausel unterstreicht der EDSB, dass je nach den Umständen (wie den gegebenen Risiken, der Komplexität des Falls, der Art der betroffenen personenbezogenen Daten und der vermutlichen Zwecke der Weiterverwendung) der für eine Lizenz erforderliche Inhalt und Detailgrad variieren kann. Es reicht daher nicht aus, lediglich zu erwähnen, dass die anzuwendenden Datenschutzvorschriften einzuhalten sind.

52. Der EDSB würde es ferner begrüßen, wenn im Vorschlag (in Artikel 8 oder auch in einem Erwägungsgrund) klargestellt würde, dass gegebenenfalls die öffentliche Stelle die Weiterverwendung personenbezogener Daten von einem "Screening" der Antragsteller abhängig machen, die Zahl der zu vergebenden Lizenzen begrenzen und die Vergabe der Lizenzen auf Antragsteller beschränken kann, die nachweislich die spezifischen Datenschutzkriterien erfüllen. Der zweite Satz des vorgeschlagenen Artikels 8 Absatz 1 sollte keinesfalls als Einschränkung dieses Ermessensspielraums gedeutet werden.

*Der Antragsteller sollte zeigen, wie er mit den Risiken umgeht*

53. Des Weiteren empfiehlt der EDSB, dass in Fällen, in denen dies mit Blick auf die Risiken für den Schutz personenbezogener Daten erforderlich ist, die Antragsteller nachweisen sollten<sup>28</sup>, dass alle Risiken im Zusammenhang mit dem Schutz personenbezogener Daten angemessen adressiert werden und der Antragsteller die Daten im Einklang mit den anzuwendenden Datenschutzvorschriften verarbeiten wird.

---

other variables, recorded separately for every person who responds; this is microdata.' (In Erhebungen und Volkszählungen sind Mikrodaten Daten, die sich auf Individuen beziehen. Bei einer Volkszählung können Alter, Wohnanschrift, Bildungsstand, Beschäftigungsstatus und viele andere Variablen für jeden einzelnen Befragten erhoben werden; dies sind Mikrodaten).

<sup>27</sup> Siehe beispielsweise die Stellungnahme des EDSB vom 22. Juli 2010 zur Vorabkontrolle der „Empirischen Analyse des Zusammenhangs zwischen Arbeitssystemvariablen und der Entscheidungsfindung“.

<sup>28</sup> Beispielsweise mit einer Datenschutzfolgenabschätzung. Zu Datenschutzfolgenabschätzungen siehe weiter oben Fußnote 24.

## *Zwecke der Weiterverwendung*

54. Der EDSB empfiehlt, im Vorschlag klarzustellen, dass abweichend von der allgemeinen Vorschrift, der zufolge eine Weiterverwendung für gewerbliche und nichtgewerbliche Zwecke erlaubt ist, die Weiterverwendung von Informationen des öffentlichen Sektors, die personenbezogene Daten enthalten, von dem Zweck abhängig gemacht werden kann, zu dem die Weiterverwendung erfolgt. In den Lizenzbedingungen sollten insbesondere die Zwecke angegeben sein, für die personenbezogene Daten verarbeitet werden dürfen, oder sollten zumindest die Zwecke genannt werden, für die die Daten ursprünglich erhoben wurden, und es sollte dort verlangt werden, dass die Weiterverwendung zu einem hiermit zu vereinbarenden Zweck zu erfolgen hat.
55. Zum Konzept des „zu vereinbarenden Zwecks“ verweist der EDSB auf Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG, der besagt: „Die Weiterverarbeitung von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken ist im allgemeinen nicht als unvereinbar mit den Zwecken der vorausgegangenen Datenerhebung anzusehen, sofern die Mitgliedstaaten geeignete Garantien vorsehen.“ Erwägungsgrund 29 besagt: „Diese Garantien müssen insbesondere ausschließen, dass die Daten für Maßnahmen oder Entscheidungen gegenüber einzelnen Betroffenen verwendet werden“.
56. Für Fälle, in denen es aufgrund der gemäß den vorstehenden Punkten 37 bis 42 durchgeführten Beurteilung angemessen ist (wenn beispielsweise, aber nicht nur dann, teilweise anonymisierte Daten für die wissenschaftliche Forschung öffentlich zugänglich gemacht werden), empfiehlt der EDSB, im Vorschlag zu fordern, dass in den Lizenzbedingungen verlangt werden sollte, dass Personen, die die Informationen weiterverwenden, keinen Versuch unternehmen, um die betroffenen Personen zu bestimmen oder die Daten für Maßnahmen oder Entscheidungen gegenüber diesen Personen zu verwenden. Dies sollte auch Dritten nicht erlaubt oder erleichtert werden.

### **3.4. Weiterverwendung durch Organisationen außerhalb der Europäischen Union**

57. Artikel 26 Absatz 1 Buchstabe f der Richtlinie 95/46/EG erlaubt eine Ausnahme von den allgemeinen Anforderungen an internationale Datenübermittlungen in Fällen, in denen „die Übermittlung aus einem [öffentlichen] Register erfolgt“.
58. Diese Ausnahme kann jedoch nicht als Rechtsgrundlage für die Übermittlung ganzer Datenbanken zum Zweck der Weiterverwendung an ein Land gedeutet werden, das unter Umständen kein angemessenes Schutzniveau bietet. Wie die Artikel 29-Datenschutzgruppe und der EDSB bereits in mehreren Stellungnahmen festgestellt haben<sup>29</sup>, gelten Ausnahmen von den Anforderungen an Übermittlungen nur fallweise und sollten keine häufigen, massiven oder strukturellen Übermittlungen zulassen.
59. Es besteht ein großer Unterschied, ob gestützt auf Artikel 26 Absatz 1 Buchstabe f öffentlich verfügbare Daten fallweise an ein Drittland übermittelt werden, das kein angemessenes Schutzniveau bietet, oder ob einem Land, das kein angemessenes Schutzniveau für personenbezogene Daten bietet, Zugang zu einer ganzen Datenbank (oder großen Teilen dieser Datenbank) gewährt und die Möglichkeit zur umfassenden

---

<sup>29</sup> Siehe Arbeitspapier der Artikel 29-Datenschutzgruppe vom 26. November 2005 über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995 (WP 114) und Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket, Punkt 224.

Weiterverwendung der Daten eingeräumt wird. Ähnlich besteht ein Unterschied, ob zum einen dem Bürger eines Drittlandes erlaubt wird, möglicherweise nach Entrichtung einer Gebühr, selektiv eine Liste von Mitgliedern der Geschäftsführung eines Unternehmens herunterzuladen, oder ob zum anderen erlaubt wird, für die Weiterverwendung in einem Drittland sämtliche Unternehmensregisterdaten eines Mitgliedstaats, einschließlich der Privatadressen und Unterschriftenproben aller eingetragenen Unternehmensvertreter, zur Verfügung zu stellen.

60. Der EDSB empfiehlt daher, in der PSI-Richtlinie ausdrücklich auf internationale Datenübermittlungen einzugehen und in diesem Zusammenhang ein angemessenes Schutzniveau oder eine andere angemessene Rechtsgrundlage für Übermittlungen in Drittländer zum Zweck der Weiterverwendung zu fordern. Weiter empfiehlt der EDSB, in dem Vorschlag vorzusehen, dass auch Lizenzbedingungen dieser Anforderung entsprechen und bei Bedarf angemessene Vertragsklauseln enthalten müssen. Allein der Verweis auf Artikel 26 Absatz 1 Buchstabe f der Richtlinie 95/46/EG ist nicht ausreichend.

### **3.5. Kosten der Anonymisierung**

*Einschlägige Bestimmung: Artikel 6*

61. Laut Vorschlag soll Artikel 6 folgendermaßen geändert werden: „Werden Gebühren für die Weiterverwendung von Dokumenten erhoben, so ist der von öffentlichen Stellen verlangte Betrag auf die durch die Vervielfältigung und Weiterverbreitung verursachten Zusatzkosten beschränkt.“
62. Diesem allgemeinen Verbot der Erhebung von Gebühren, die über die durch die Vervielfältigung und Verbreitung verursachten Zusatzkosten hinausgehen, folgt eine Reihe von Ausnahmen u. a. für Bibliotheken, Museen und Archive sowie für bestimmte andere öffentliche Stellen, die ihre Kosten aus der Nutzung ihrer Rechte des geistigen Eigentums decken. Für Informationen des öffentlichen Sektors, die personenbezogene Daten enthalten, sind keine konkreten Ausnahmen vorgesehen.

*Ausnahme für Anonymisierungskosten*

63. In manchen Fällen kann die Anonymisierung von Dokumenten, die im Besitz öffentlicher Stellen sind, ein komplexes, zeitaufwändiges und kostspieliges Unterfangen sein, das besonderes Fachwissen erfordert, über das möglicherweise nicht alle öffentlichen Stellen verfügen. Eine solche Anonymisierung mag jedoch häufig aufgrund bestehender Risiken erforderlich sein und kann sich auch in Anbetracht des Werts teilweise oder vollständig anonymisierter Daten lohnen, die dann zur Weiterverwendung zur Verfügung gestellt werden können. Wird öffentlichen Stellen erlaubt, sich diese Kosten erstatten zu lassen, trägt dies dazu bei, dass die Anonymisierung sorgfältig durchgeführt wird, und dies wiederum kann zu einem höheren Datenschutzniveau und gleichzeitig zu mehr Transparenz und Verfügbarkeit zur Weiterverwendung führen.
64. Aus diesen Gründen sollte in Erwägung gezogen werden, in Artikel 6 Absatz 1 eine weitere Ausnahme vorzusehen, der zufolge der öffentlichen Stelle erlaubt wird, dem Lizenznehmer zumindest angemessene Kosten in Rechnung zu stellen, die ihr bei der Vorverarbeitung (z. B. Digitalisierung), Aggregierung und/oder (teilweisen oder vollständigen) Anonymisierung der zur Weiterverwendung angebotenen

personenbezogenen Daten entstehen, sofern der Einsatz solcher Techniken aufgrund der größeren Risiken gerechtfertigt ist, die aus dem Angebot solcher Daten zur Weiterverwendung entstehen.

65. Die Gebührenerhebung im Zusammenhang mit der Weiterverwendung von Dokumenten darf natürlich nicht mit der Erhebung von Gebühren für den Zugang zu Dokumenten nach den einschlägigen Rechtsvorschriften verwechselt werden. Um das hier bestehende Konfliktpotenzial möglichst klein zu halten, könnte es sich als hilfreich erweisen, wenn der Vorschlag (beispielsweise in einem Erwägungsgrund) klarstellen würde, dass diese Ausnahme unbeschadet der nationalen Rechtsvorschriften über den Zugang zu Dokumenten gewährt wird, denen zufolge der Zugang zu Dokumenten kostenlos oder zu einem Preis gewährt wird, der beispielsweise nicht die „Zusatzkosten“ übersteigen darf, „die durch die Vervielfältigung und Verbreitung“ der Dokumente verursacht werden.

### **3.6. Weitere Leitlinien für Anonymisierung und Lizenzen; Konsultation der Artikel 29-Datenschutzgruppe**

66. Der EDSB empfiehlt der Kommission, in einem Kommissionsdokument (Empfehlung der Kommission, Durchführungsrechtsakt oder Arbeitsunterlage) weitere Leitlinien zu den Datenschutzaspekten der PSI-Richtlinie, insbesondere zu den Themen Anonymisierung und Lizenzen, zu formulieren. Besonders hilfreich wäre in diesem Zusammenhang ein Muster für angemessene Datenschutzklauseln in Lizenzen. Der EDSB empfiehlt ferner, im Vorschlag ausdrücklich auf solche Leitlinien Bezug zu nehmen und anzugeben, in welcher Form (z. B. Durchführungsrechtsakte) sie bereitgestellt werden.
67. Der EDSB stellt ferner fest, dass die Artikel 29-Datenschutzgruppe auch weiterhin eine hilfreiche Rolle spielen könnte; sie könnte ihr Sachverständigenwissen einbringen und für mehr Kohärenz in diesem Bereich sorgen, insbesondere indem sie bewährte Vorgehensweisen aus den Mitgliedstaaten zusammenstellt und, gestützt auf nationale Erfahrungen, harmonisierte Ansätze entwickelt. Wie bereits unter Punkt 18 angemerkt, stand die Weiterverwendung von Informationen des öffentlichen Sektors schon 2003 auf der Tagesordnung der Artikel 29-Datenschutzgruppe. In Anbetracht der derzeitigen Überarbeitung der PSI-Richtlinie und der bisherigen Erfahrungen sowie der laufenden Überarbeitung des EU-Datenschutzrahmens könnte sich die Arbeitsgruppe erneut mit dem Thema befassen und u. a. im Detail auf die Themen Anonymisierung und Lizenzen eingehen.

## **4. ANALYSE DES KOMMISSIONSBESCHLUSSES**

68. Der EDSB bedauert, dass er vor der Annahme des Beschlussentwurfs nicht konsultiert wurde. Da der Beschluss bereits angenommen wurde, wird der EDSB nur kurz auf die Punkte eingehen, die hätten verbessert werden können. Er schlägt vor, seine Anmerkungen einstweilen zumindest bei der Auslegung der Bestimmungen des Beschlusses zu berücksichtigen. In einer zweiten Phase sollte bei einer Überprüfung des Beschlusses eine Änderung erwogen werden.
69. Erstens empfiehlt der EDSB, den Begriff „öffentliche Daten“ in Artikel 2 Buchstabe a unter Berücksichtigung der geltenden EU-Rechtsvorschriften über den Zugang zu

Dokumenten und über den Datenschutz sowie der Rechtsprechung der europäischen Gerichte genauer zu definieren.

70. Ferner empfiehlt der EDSB, in dem Beschluss klarer zum Ausdruck zu bringen, ob er auch für andere als die personenbezogenen Daten gilt, die nach den EU-Rechtsvorschriften über den Zugang zu Dokumenten offen gelegt werden dürfen. Gemäß Artikel 2 Buchstabe c scheint dies ausgeschlossen zu sein, doch wäre es der Rechtssicherheit zuträglich, wenn dies klargestellt würde.
71. Schließlich gelten die den Vorschlag betreffenden Kommentare zu Anonymisierung (Abschnitt 3.2), Lizenzen (Abschnitt 3.3), internationale Übermittlungen (Abschnitt 3.4) und Kosten der Anonymisierung und Aggregation (Abschnitt 3.5) sinngemäß auch für den Beschluss.

## **5. SCHLUSSFOLGERUNGEN**

72. Die Weiterverwendung von Informationen des öffentlichen Sektors, die personenbezogene Daten enthalten, kann beträchtliche Vorteile mit sich bringen, birgt aber auch erhebliche Risiken für den Schutz personenbezogener Daten. In Anbetracht dieser Risiken empfiehlt der EDSB, im Vorschlag klarer festzulegen, in welchen Situationen und vorbehaltlich welcher Garantien beantragt werden kann, Informationen, die personenbezogene Daten enthalten, zur Weiterverwendung zur Verfügung zu stellen. Der Vorschlag sollte insbesondere
- klarer den Umfang der Anwendbarkeit der PSI-Richtlinie auf personenbezogene Daten festlegen (Abschnitt 3.1);
  - von der betreffenden öffentlichen Stelle die Durchführung einer Beurteilung verlangen, bevor irgendwelche Informationen des öffentlichen Sektors, die personenbezogene Daten enthalten, zur Weiterverwendung zur Verfügung gestellt werden (Abschnitt 3.1);
  - gegebenenfalls verlangen, dass die Daten vollständig oder teilweise anonymisiert werden und in den Lizenzbedingungen ausdrücklich die erneute Bestimmung natürlicher Personen und die Weiterverwendung personenbezogener Daten für Zwecke verboten werden, die die betroffenen Personen individuell berühren könnten (Abschnitte 3.2 und 3.3);
  - fordern, dass die Lizenzbedingungen für die Weiterverwendung von Informationen des öffentlichen Sektors eine Datenschutzklausel enthalten, sofern personenbezogene Daten verarbeitet werden (Abschnitt 3.3);
  - erforderlichenfalls die Risiken für den Schutz personenbezogener Daten prüfen, von den Antragstellern einen Nachweis (mit Hilfe einer Datenschutzfolgenabschätzung oder anderer Mittel) darüber verlangen, dass mit allen Risiken für den Schutz personenbezogener Daten angemessen umgegangen wird und dass der Antragsteller die Daten im Einklang mit den geltenden Datenschutzvorschriften verarbeiten wird (Abschnitt 3.3);
  - klarstellen, dass abweichend von der allgemeinen Vorschrift, die eine Weiterverwendung zu gewerblichen und nichtgewerblichen Zwecken erlaubt, die Weiterverwendung von ihrem Zweck abhängig gemacht werden kann (Abschnitt 3.3).

73. Darüber hinaus schlägt der EDSB vor,

- in Erwägung zu ziehen, ob nicht Kosten für die Vorverarbeitung (wie Digitalisierung), Anonymisierung und Aggregation gegebenenfalls dem Lizenznehmer in Rechnung gestellt werden können (Abschnitt 3.5), und
- dass die Kommission hauptsächlich zu den Themen Anonymisierung und Lizenzen weitere Leitlinien ausarbeitet und die Artikel 29-Datenschutzgruppe hierzu konsultiert (Abschnitt 3.6).

Brüssel, den 18. April 2012

**(unterzeichnet)**

Peter HUSTINX  
Europäischer Datenschutzbeauftragter