ARTIKEL-29-DATENSCHUTZGRUPPE

1021/00/DE
WP 207

Stellungnahme 6/2013 zu den Offenen Daten ('Open Data') und der Weiterverwendung von Informationen des öffentlichen Sektors ('PSI')

Angenommen am 5. Juni 2013

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 sowie auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. Einleitung

1.1. Überarbeitung der PSI-Richtlinie

Am 26. Juni 2013 hat die Europäische Union die Richtlinie 2013/37/EU des Europäischen Parlaments und des Rates ('PSI-Änderungsrichtlinie') zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors ('PSI-Richtlinie') erlassen.[1]

Die PSI-Richtlinie dient der Erleichterung der Weiterverwendung von Informationen des öffentlichen Sektors im Wege der Angleichung der Bedingungen für diese Weiterverwendung in der gesamten Europäischen Union und der Beseitigung der unnötigen Hemmnisse für diese Weiterverwendung im Binnenmarkt.

Im ursprünglichen Wortlaut von 2003 harmonisierte die PSI-Richtlinie die Bedingungen für die Weiterverwendung, verlangte aber von den öffentlichen Stellen nicht, Daten für die Weiterverwendung zur Verfügung zu stellen. Die Frage, ob Daten für die Weiterverwendung zur Verfügung gestellt werden sollen, wurde fakultativ angegangen: Die Entscheidung darüber wurde den Mitgliedstaaten und den betreffenden öffentlichen Stellen überlassen. Dies führte im Ergebnis dazu, dass viele öffentliche Stellen überall in Europa sich einfach dafür entschieden, die Weiterverwendung ihrer Informationen nicht zu gestatten.

Vor diesem Hintergrund ist eines der politischen Leitziele der PSI-Änderungsrichtlinie die Einführung des Grundsatzes, dass alle öffentlichen Informationen (d. h. alle im öffentlichen Sektor vorhandenen Informationen, die nach innerstaatlichem Recht öffentlich zugänglich sind) sowohl für kommerzielle als auch für nichtkommerzielle Zwecke weiterverwendet werden können. In bestimmten Fällen, so auch aus Gründen des Datenschutzes, gelten für den Anwendungsbereich der geänderten PSI-Richtlinie gewisse Ausnahmen.[2]

Die geänderte Datenschutzrichtlinie schreibt den öffentlichen Stellen jetzt zwingend vor, die Weiterverwendung aller bei ihnen vorhandenen öffentlichen Informationen zu gestatten. Wie weiter unten noch dargelegt wird, verpflichtet sie die öffentlichen Stellen jedoch nicht zur Offenlegung von personenbezogenen Informationen. Die Weiterverwendung von Informationen ist nur vorgesehen, wenn diese bereits nach innerstaatlichem Recht öffentlich zugänglich sind, und auch nur dann, wenn die Weiterverwendung keinerlei Vorschriften des geltenden Datenschutzrechts verletzen kann.

1 ABl. L 175 vom 27.6.2013, S. 1.

2 Zum Anwendungsbereich der geänderten PSI-Richtlinie und der Datenschutzvorschriften siehe weiter unten Abschnitt V.

Relevant sind auch andere neue Bestimmungen der PSI-Änderungsrichtlinie, die den Anwendungsbereich der PSI-Richtlinie auf Bibliotheken (einschließlich Hochschulbibliotheken), Archive und Museen erweitern.

Angesichts vorstehender Erwägungen ist die geänderte PSI-Richtlinie geeignet, die Zugriffsmöglichkeiten auf die bei öffentlichen Stellen vorhandenen Informationen deutlich zu verbessern.

1.2. Weiterverwendung von Informationen des öffentlichen Sektors (PSI) und personenbezogene Daten

Bei den Initiativen für eine Weiterverwendung von Informationen des öffentlichen Sektors geht es normalerweise darum, (i) ganze Datenbanken verfügbar zu machen, (ii) in standardisierter elektronischer Form, (iii) jeglichem Antragsteller ohne Prüfverfahren, (iv) unentgeltlich (bzw. gegen auf die Grenzkosten beschränkte Gebühren) und (v) für jegliche kommerzielle und nichtkommerzielle Zwecke und ohne Bedingungen (bzw. zu nichteinschränkenden Bedingungen, gegebenenfalls im Rahmen einer Lizenz)[3].

Dies bringt mitunter Vorteile, die zu mehr Transparenz und zu einer innovativen Weiterverwendung von Informationen des öffentlichen Sektors führen. Jedoch ist die daraus erwachsende größere Zugriffsmöglichkeit auf Informationen auch nicht ohne Risiken.

Wann immer es um personenbezogene Daten geht, muss das Datenschutzrecht, um diese Risiken möglichst gering zu halten, eine Orientierungshilfe für die Entscheidung bieten, welche personenbezogenen Daten für eine Weiterverwendung bereitgestellt werden bzw. nicht bereitgestellt werden können und welche Maßnahmen zum Schutz personenbezogener Daten zu ergreifen sind. In allen Fällen, in denen der Schutz der Privatsphäre oder der personenbezogenen Daten auf dem Spiel steht, muss ein ausgewogenes Gesamtkonzept verfolgt werden. Einerseits sollten die Vorschriften zum Schutz personenbezogener Daten kein unangemessenes Hemmnis für die Entwicklung des Weiterverwendungsmarktes darstellen. Andererseits muss dem Recht auf Schutz der personenbezogenen Daten und dem Recht auf Privatsphäre Genüge getan werden. Dabei muss unbedingt betont werden, dass die Schwerpunktsetzung für 'offene Daten' vom Konzept her auf der Transparenz und der Rechenschaftspflicht der öffentlichen Stellen sowie dem Wirtschaftswachstum und nicht auf der Durchsichtigkeit des einzelnen Bürgers liegt.

Bei der Anwendung der PSI-Richtlinie und des Datenschutzrechts auf die Weiterverwendung von personenbezogenen Daten trifft eine öffentliche Stelle voraussichtlich eine dieser drei verschiedenen Entscheidungen:

1. Die Entscheidung, personenbezogene Informationen nicht für die Weiterverwendung gemäß der PSI-Richtlinie bereitzustellen;
2. die Entscheidung, personenbezogene Informationen in eine anonymisierte Form (für gewöhnlich in aggregierte statistische Daten) umzuwandeln[4] und nur diese anonymisierten Daten für die Weiterverwendung bereitzustellen;

---

[3] Gemäß Artikel 8 Absatz 11 der geänderten PSI-Richtlinie dürfen die Lizenz bzw. deren 'Bedingungen die Möglichkeiten der Weiterverwendung nicht unnötig einschränken und nicht der Behinderung des Wettbewerbs dienen'.

[4] Zur Weiterverwendung von aggregierten und anonymisierten Datensätzen, die von personenbezogenen Daten abgeleitet wurden, siehe weiter unten Abschnitt VI.

3. die Entscheidung, personenbezogene Informationen für die Weiterverwendung bereitzustellen (gegebenenfalls unter spezifischen Bedingungen und vorbehaltlich angemessener Sicherheits- und Schutzmaßnahmen).

II. Zielsetzung dieser Stellungnahme

2.1. Kohärente Handlungsempfehlungen und bewährte Vorgehensweisen

Diese Stellungnahme soll dabei helfen, ein gemeinsames Verständnis des geltenden Rechtsrahmens sicherzustellen, und kohärente Handlungsempfehlungen sowie Beispiele für bewährte Vorgehensweisen dafür anbieten, wie die PSI-Richtlinie (in der geänderten Fassung) in Bezug auf die Verarbeitung personenbezogener Daten umzusetzen ist.

Mit dieser Stellungnahme soll hingegen nicht versucht werden, innerstaatliche Konzepte für das Maß an Transparenz, die nationale Gesetzgebung über den Zugang zu Dokumenten und die Verfügbarkeit von Informationen nach innerstaatlichem Recht zu harmonisieren. Allerdings weichen die nationalen Umsetzungsvorschriften für die PSI-Richtlinie und die nationalen Auslegungen der Richtlinie 95/46/EG[5] in Bezug auf die Weiterverwendung von Informationen des öffentlichen Sektors bisweilen in einem Maße voneinander ab, das über das hinausgeht, was notwendig sein mag, um bei den nationalen Zugangsregelungen und den verschiedenen Transparenzniveaus für Vielfalt zu sorgen.

Diesbezüglich veranschaulichen die vom Europäischen Thematischen Netz LAPSI ausgearbeiteten grundsatzpolitischen Empfehlungen zur Privatsphäre vom September 2012 deutlich die unnötigen Unterschiede in der Art und Weise, wie die PSI-Richtlinie in Bezug auf den Schutz personenbezogener Daten in den Mitgliedsaaten umgesetzt wurde.[6] Die PSI-Richtlinie selbst enthält die Warnung, dass die rechtlichen Unterschiede und Unsicherheiten mit der Weiterentwicklung der Informationsgesellschaft, die bereits zu einer wesentlich stärkeren grenzüberschreitenden Informationsnutzung geführt hat, an Bedeutung gewinnen.[7]

Mangels eines kohärenten Gesamtkonzepts kann die Position der betreffenden natürlichen Personen geschwächt werden. Dies kann auch unnötige regulatorische Belastungen für grenzüberschreitend tätige Wirtschaftsbeteiligte und andere Organisationen mit sich bringen und somit ein Hemmnis für die Entwicklung eines gemeinsamen europäischen Marktes für die Weiterverwendung von Informationen des öffentlichen Sektors darstellen. Denn einerseits muss den betroffenen Personen versichert werden, dass ihre Daten ungeachtet ihrer Übermittlung in einen anderen Mitgliedstaat zu Zwecken der Weiterverwendung gleichbleibend geschützt werden. Andererseits sollte eine ungebührliche Komplexität und Fragmentierung vermieden werden, auch um den freien Fluss von personenbezogenen Daten in ganz Europa zu ermöglichen, was ein weiteres Leitziel der Richtlinie 95/46/EG darstellt.

---

[5] 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 (ABl. L 281 vom 23.11.1995, S. 31).

[6] LAPSI ist das von der Europäischen Kommission geförderte Europäische Thematische Netz für die 'rechtlichen Aspekte der Informationen des öffentlichen Sektors', siehe: http://www.lapsi-project.eu/. Die grundsatzpolitischen Empfehlungen sind abrufbar unter: http://www.lapsi-project.eu/lapsifiles/lapsi_privacy_policy.pdf.

[7] Siehe Erwägungsgrund Nr. 7.

2.2. Notwendigkeit der Aktualisierung der Stellungnahme 7/2003

Die PSI-Änderungsrichtlinie kommt zehn Jahre nach Annahme der PSI-Richtlinie im Jahr 2003. Zu dieser Zeit nahm die Artikel-29-Datenschutzgruppe eine Stellungnahme zu den Datenschutzbelangen betreffend Informationen des öffentlichen Sektors an ('Stellungnahme 7/2003')[8]. Während die wichtigsten Grundsätze, die in dieser Stellungnahme 7/2003 dargelegt wurden, nach wie vor stichhaltig sind, rechtfertigen die technologische und sonstige Entwicklung auf dem Gebiet der Informationen des öffentlichen Sektors (PSI) und des Datenschutzes, einschließlich der auf beiden Gebieten vorgeschlagenen gesetzlichen Änderungen, die derzeitigen Anstrengungen zur Aktualisierung und Ergänzung der Stellungnahme von 2003.

Ferner kann diese Stellungnahme nun auch andere jüngste und noch laufende Anstrengungen zur Bereitstellung von weiteren Handlungsempfehlungen berücksichtigen, so vor allem

- die Stellungnahme des Europäischen Datenschutzbeauftragten('EDSB') vom 18. April 2012 zum 'Offene-Daten-Paket' der Europäischen Kommission[9];
- die Stellungnahme 3/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung[10];
- die laufenden Arbeiten in der Untergruppe 'Technologie' der Artikel-29-Datenschutzgruppe zu Anonymisierungstechniken[11];
- die Arbeiten in einigen Mitgliedstaaten zu den Themenbereichen Anonymisierung und Risikobewertung;[12] und
- die einschlägige Rechtsprechung und Entscheidungspraxis einiger Mitgliedstaaten zur Interessenabwägung zwischen der Weiterverwendung von Informationen des öffentlichen Sektors und dem Schutz personenbezogener Daten[13].

III. Schwerpunktsetzung und Struktur der Stellungnahme

Die Stellungnahme 7/2003 konzentrierte sich auf den Grundsatz der Zweckbindung[14], sprach aber auch andere Themenbereiche an, wie z. B. die rechtliche Zulässigkeit der Offenlegung und

---

[8] Siehe Stellungnahme 7/2003 der Artikel-29-Datenschutzgruppe zur Weiterverwendung von Informationen des öffentlichen Sektors und zum Schutz personenbezogener Daten - Interessenabwägung – angenommen am 12. Dezember 2003 (WP 83). Siehe dazu auch zwei frühere damit zusammenhängende Stellungnahmen der Artikel-29-Datenschutzgruppe: Stellungnahme 3/1999 betreffend die Informationen des öffentlichen Sektors und den Schutz personenbezogener Daten, angenommen am 3. Mai 1999 (WP 20) sowie Stellungnahme 5/2001 zum Sonderbericht des Europäischen Bürgerbeauftragten , angenommen am 17. Mai 2001.

[9] Stellungnahme des Europäischen Datenschutzbeauftragten (EDSB) vom 18. April 2012 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; abzurufen unter: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-04-18_Open_data_DE.pdf.

[10] Stellungnahme 3/2013 der Artikel-29-Datenschutzgruppe zur Zweckbindung, angenommen am 2. April 2013 (WP 203).

[11] Eine Stellungnahme zu diesem Thema dürfte im zweiten Halbjahr 2013 angenommen werden.

[12] Siehe beispielsweise den von der nationalen Datenschutzbehörde des Vereinigten Königreichs (Information Commissioner's Office) im November 2012 herausgegebenen Anonymisierungs-Verfahrenskodex „Anonymisierung: Verfahrenskodex für das Risikomanagement beim Datenschutz" ('Anonymisation: Managing data protection risk code of practice') und die von der französischen Datenschutzbehörde im Juni 2012 herausgegebenen Handlungsempfehlungen für die Risikoanalyse.

[13] Siehe beispielsweise die grundsatzpolitischen Empfehlungen des LAPSI vom September 2012 (S. 4-14).

[14] Siehe Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG.

Weiterverwendung von Informationen des öffentlichen Sektors, den besonderen Schutz sensibler Daten, die Übermittlung in Drittländer, die Datenqualität und die Rechte betroffener Personen. Diese Feststellungen haben nach wie vor Gültigkeit. Unter Berücksichtigung der bereits vorhandenen Arbeitsergebnisse aktualisiert und ergänzt die vorliegende Stellungnahme gegebenenfalls nur noch die Schlussfolgerungen aus der Stellungnahme 7/2003 im Lichte der neuen rechtlichen und technologischen Entwicklungen.

Abschnitt IV verdeutlicht, dass die Verpflichtung nach der geänderten PSI-Richtlinie, alle Dokumente weiterverwendbar zu machen, unbeschadet der Datenschutzvorschriften besteht, und betont, wie wichtig die Berücksichtigung des Datenschutzes bereits in der Planungs- und Entwicklungsphase ('data protection by design') wie auch im Fall von bestehenden Verarbeitungssystemen seine Berücksichtigung nach Maßgabe der datensparsamsten Voreinstellungen ('data protection by default') und ferner 'Datenschutz-Folgenabschätzungen' sind, um sicherstellen zu können, dass auf die Belange des Datenschutzes eingegangen wird, bevor personenbezogene Daten für eine Weiterverwendung bereitgestellt werden.

Abschnitt V gibt anhand von erläuternden Beispielen Orientierungshilfen, welche Art von personenbezogenen Daten unter den Anwendungsbereich der PSI-Richtlinie fallen kann.

Abschnitt VI konzentriert sich auf die bei Initiativen für eine Weiterverwendung von Informationen des öffentlichen Sektors derzeit geläufigsten Situationen: aggregierte statistische Daten, die aus personenbezogenen Daten abgeleitet wurden, werden in aggregierter und anonymisierter Form bereitgestellt. Zu den Beispielsfällen gehören aggregierte statistische Daten zu der Kriminalitätsrate, den Ausgaben der öffentlichen Hand oder der Lernerfolgsquote von Schulkindern in verschiedenen geografischen Regionen oder Bildungseinrichtungen. Da es sich hierbei um das gängigste Szenario der Weiterverwendung von Informationen des öffentlichen Sektors, die personenbezogene Daten beinhalten, handelt, ist ein erheblicher Teil der vorliegenden Stellungnahme diesem Szenario gewidmet. Das zentrale Anliegen für den Datenschutz besteht hier darin, die effektive Aggregation und Anonymisierung sicherzustellen und das Risiko, dass personenbezogene Daten aus aggregierten Datensätzen identifiziert und wiedererkannt werden können, möglichst gering zu halten.

In Abschnitt VII werden – etwas weniger ausführlich – Situationen erörtert, in denen personenbezogene Daten öffentlich zugänglich gemacht werden und damit potenziell für eine Weiterverwendung zur Verfügung stehen. Zwar ist dies derzeit nicht das typische Szenario von Initiativen für eine Weiterverwendung von Informationen des öffentlichen Sektors, doch ist unbedingt zu bedenken, dass öffentliche Stellen personenbezogene Daten mehr und mehr öffentlich zugänglich machen, häufig auch im Internet. Hier wird oft von direkt identifizierbaren personenbezogenen Daten gesprochen, so z. B. bei den Angaben im Grundbuch über den Eigentümer einer bestimmten Immobilie, den Erklärungen zu den Einkünften aus Kapital oder aus Vergütungen bei bestimmten Beamten bzw. zu den Ausgaben der Parlamentsabgeordneten. Hier stellt sich die Frage, in welchen Ausmaßen, zu welchen Zwecken, unter welchen Bedingungen und vorbehaltlich welcher Schutz- und Sicherheitsmaßnahmen diese Daten für eine Weiterverwendung bereitgestellt werden dürfen. Es muss auch unbedingt klargestellt sein, ob diese Daten unter die Bestimmungen der PSI-Richtlinie fallen.

In diesem Zusammenhang muss hervorgehoben werden, dass jegliche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, unabhängig davon, ob sie öffentlich zugänglich sind oder nicht, personenbezogene Daten darstellen. Daher unterliegen der Zugriff auf personenbezogene Daten und deren Weiterverwendung, auch wenn sie öffentlich zugänglich gemacht wurden (z. B. durch Veröffentlichung dieser Daten im Internet) nach wie vor dem einschlägigen Datenschutzrecht.

Einige andere spezielle Szenarios, wie z. B. im Falle von Forschungsdaten und historischen Archiven – die ab jetzt in den Anwendungsbereich der PSI-Richtlinie fallen – werden in den Abschnitten VIII und IX kurz angesprochen.

In Abschnitt X wird die Frage der Lizenzvergabe für Informationen des öffentlichen Sektors und die Notwendigkeit erörtert, gegebenenfalls eine Datenschutzklausel in die Lizenzerteilung aufzunehmen.

Abschnitt XI schließt mit einer Reihe von Schlussfolgerungen und Empfehlungen.

IV. Nicht alle 'öffentlich zugänglichen' personenbezogenen Daten sollten für eine Weiterverwendung zur Verfügung gestellt werden

4.1. Die Verpflichtung zur Weiterverwendbarkeit aller Dokumente im Rahmen der PSI-Richtlinie besteht unbeschadet der Datenschutzvorschriften

Die 2003 erlassene PSI-Richtlinie hat den öffentlichen Stellen keinerlei Verpflichtung auferlegt, die Weiterverwendung von Informationen des öffentlichen Sektors zu gestatten. Die Entscheidung, die Weiterverwendung zu genehmigen oder zu untersagen, verblieb (nach Maßgabe des jeweiligen innerstaatlichen Regelungsrahmens für Transparenz und Zugang) bei den Mitgliedstaaten bzw. bei der betreffenden öffentlichen Stelle. Die Stellungnahme 7/2003 wurde im Lichte dieser 'Nicht-Verpflichtung' angenommen. In Abschnitt II 2 a) (cc) dieser Stellungnahme wird festgestellt: "Hervorzuheben ist aber, dass die Weiterverwendungs-Richtlinie als eine solche rechtliche Verpflichtung, die es zu erfüllen gilt, nicht in Anspruch genommen werden kann, weil diese Richtlinie keine Verpflichtung zur Weitergabe personenbezogener Daten schafft".

Mit der PSI-Änderungsrichtlinie wird die Analyse zwar komplizierter, doch bleibt die endgültige Schlussfolgerung dieselbe.

Nach Artikel 3 Absatz 1 der geänderten PSI-Richtlinie gilt Folgendes: "Vorbehaltlich des Absatzes 2 stellen die Mitgliedstaaten sicher, dass die Dokumente, auf die diese Richtlinie gemäß Artikel 1 anwendbar ist, gemäß den Bedingungen der Kapitel III und IV für gewerbliche und nichtgewerbliche Zwecke weiterverwendet werden können". Solange die Weiterverwendung nicht aus den in Artikel 1 genannten Gründen (aus von den Zugangsregelungen der Mitgliedstaaten abgeleiteten Gründen und speziell auch aus Gründen des Schutzes von personenbezogenen Daten) untersagt werden kann, muss die Weiterverwendung gestattet werden.

Gleichzeitig enthält der Erwägungsgrund 21 der PSI-Richtlinie die folgende Feststellung: "Diese Richtlinie sollte unter uneingeschränkter Beachtung der Grundsätze des Schutzes personenbezogener Daten […] durchgeführt und angewandt werden". Ferner bestimmt Artikel 1 Absatz 4: "Diese Richtlinie hat keinerlei Auswirkungen auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten".

Kombiniert man diese Aussagen in einer Gesamtschau, so bedeuten die Bestimmungen zusammengenommen, dass der 'Grundsatz der Weiterverwendbarkeit' keinen Automatismus entfaltet, wenn das Recht auf Schutz von personenbezogenen Daten auf dem Spiel steht, und auch nicht die einschlägigen Bestimmungen des Datenschutzrechts aushebelt. Wenn Dokumente, die sich im Besitz öffentlicher Stellen befinden, personenbezogene Daten enthalten, so fällt ihre Weiterverwendbarkeit in den Anwendungsbereich der Richtlinie 95/46/EG und unterliegt somit nach wie vor dem einschlägigen Datenschutzrecht.

Folglich kann sich die öffentliche Stelle in Fällen, in denen die Weiterverwendung personenbezogene Daten mitumfassen würde, nicht systematisch auf die Notwendigkeit berufen, die PSI-Richtlinie als Rechtsgrund für die Bereitstellung der Daten zu Zwecken ihrer Weiterverwendung einhalten zu müssen.[15]

4.2. Wichtigkeit einer Datenschutz-Folgenabschätzung vor der Offenlegung von Daten zu Zwecken der Weiterverwendung

Angesichts der potenziellen Risiken, die eine Weiterverwendung von Informationen des öffentlichen Sektors in sich birgt, und insbesondere der Tatsache, dass sobald einmal personenbezogene Daten zu Zwecken der Weiterverwendung öffentlich zugänglich gemacht wurden, es sehr schwer sein wird, die Nutzung solcher Daten wirksam zu kontrollieren, betont die Datenschutzgruppe die Notwendigkeit, die Grundsätze der Berücksichtigung des Datenschutzes bereits in der Planungs- und Entwicklungsphase ('data protection by design') wie auch im Fall von bestehenden Verarbeitungssystemen seiner Berücksichtigung nach Maßgabe der datensparsamsten Voreinstellungen ('data protection by default') einzuhalten und sicherzustellen, dass auf die Datenschutzbelange schon in einem sehr frühen Stadium eingegangen wird. Insbesondere empfiehlt die Artikel-29-Datenschutzgruppe mit Nachdruck, dass von der öffentlichen Stelle eine gründliche Datenschutzfolgenabschätzung durchgeführt wird, bevor sie personenbezogene Daten zu Zwecken der Weiterverwendung bereitstellt. Auch die Mitgliedstaaten sollten erwägen, solche Folgenabschätzungen im Rahmen der innerstaatlichen Gesetzgebung zwingend vorzuschreiben oder wenigstens als bewährte Vorgehensweise zu fördern. Auch wenn dies nach nationalem Recht nicht ausdrücklich vorgeschrieben ist, sollten die öffentlichen Stellen vor der Offenlegung von Informationen und vor ihrer Entscheidung, diese Informationen zu Zwecken der Weiterverwendung zur Verfügung zu stellen, in jedem Fall eine gründliche Folgenabschätzung vornehmen, anhand derer sie feststellen können, ob personenbezogene Daten zu Zwecken der Weiterverwendung bereitgestellt werden dürfen und wenn ja, unter welchen Bedingungen und nach Maßgabe welcher speziellen Datenschutzgarantien eine Weiterverwendung statthaft ist.

Anhand der Folgenabschätzung sollte unter anderem die Rechtsgrundlage für die Offenlegung (und die mögliche Rechtsgrundlage für die Weiterverwendung) bestimmt, die Einhaltung der Grundsätze der Zweckbindung, der Verhältnismäßigkeit und der Datensparsamkeit bewertet und der für sensible Daten erforderliche besondere Schutz berücksichtigt werden. Bei der Durchführung dieser Bewertung gilt es, die potenziellen Auswirkungen auf die betroffenen Personen sorgfältig zu berücksichtigen.

Diese Folgenabschätzung sollte eine Entscheidungshilfe dafür bieten, ob überhaupt und wenn ja, dann welche personenbezogenen Daten nach Maßgabe welcher Datenschutzgarantien für die konkrete Weiterverwendung bereitgestellt werden dürfen.[16] Hervorzuheben ist, dass der Vorschlag für die Datenschutz-Grundverordnung[17] Datenschutz-Folgenabschätzungen anregt und in einigen Fällen

---

[15] Die Datenschutzgruppe möchte ebenfalls klarstellen, dass die PSI-Richtlinie als solche auch aus der Sicht des Weiterverwenders keinen Rechtsgrund für die Verarbeitung von Daten schafft. (Zu den Rechtsgründen siehe Stellungnahme 7/2003 sowie Abschnitt 7.5. weiter unten.)

[16] Führt die Folgenabschätzung zu der Entscheidung, zu Zwecken der Weiterverwendung keine personenbezogenen Daten als solche sondern vielmehr aus personenbezogenen Daten abgeleitete und anonymisierte Datensätze bereitzustellen, dann sollte eine Wiedererkennbarkeits-Risikobewertung durchgeführt werden. Siehe dazu Anschnitt VI zur Anonymisierung und zur Risikobewertung hinsichtlich der Identifizierbarkeit/Wiedererkennbarkeit.

[17] Am 25. Januar 2012 hat die Kommission ein Paket zur Reform des europäischen Datenschutzrahmens angenommen. Dieses Paket umfasst (i) die 'Mitteilung zum europäischen Datenschutzrahmen' (KOM(2012)9 endgültig), (ii) den 'Vorschlag für die Datenschutz-Grundverordnung' (KOM(2012)11 endgültig) und (iii) den 'Vorschlag für die Datenschutzrichtlinie' (KOM(2012)10 endgültig).

sogar vorschreibt, da sie ein wichtiges Instrument zur Sicherstellung der Rechenschaftspflicht und Verantwortlichkeit des für die Verarbeitung der Daten Verantwortlichen sind.[18]

Wann immer es möglich ist, sollte die Analyse vor der Weiterverwendungsentscheidung auf der Grundlage einer sachkundigen Debatte erfolgen, an der sich die verschiedenen Interessenvertreter beteiligen, so nicht nur der für die Verarbeitung der Daten Verantwortliche, der die Daten freigeben möchte, sondern auch diejenigen, die die Daten verlangen und daher die Zusammenhänge für die Diskussion liefern, wie auch die Vertreter der natürlichen Personen, um deren personenbezogene Daten es geht (z. B. Verbraucherschutzorganisationen, Organisationen zum Schutz der Patientenrechte, Lehrergewerkschaften). Kommt kein klares Ergebnis dabei heraus, so können die zuständige Datenschutzbehörde und die für die Informationsfreiheit verantwortlichen nationalen Behörden unter Umständen Handlungsempfehlungen geben.

Die Mitgliedstaaten sollten auch erwägen, eine Förderung für Wissensnetze/Kompetenzzentren auf die Beine zu stellen und zu gewähren und damit den Austausch und die gemeinsame Nutzung von bewährten Verfahrensweisen im Zusammenhang mit der Anonymisierung und den offenen Daten zu ermöglichen. Diese können besonders wichtig sein für kleinere öffentliche Stellen, die mitunter nicht über das nötige Fachwissen verfügen, um Anonymisierungen, Datenschutz-Folgenabschätzungen und Risikobewertungen/-tests hinsichtlich der Identifizierbarkeit/Wiedererkennbarkeit durchführen zu können.[19]

Schließlich wird auch nachdrücklich empfohlen, eine Folgenabschätzung vorzunehmen, bevor neue Rechtsvorschriften in Kraft treten, die eine Offenlegung personenbezogener Daten vorschreiben.

V. Anwendungsbereich der PSI-Richtlinie: Ausnahmen von den Gründen für den Schutz von personenbezogenen Daten

Dieser Abschnitt bietet Orientierungshilfen zum Anwendungsbereich der PSI-Richtlinie und insbesondere zu den Ausnahmen von den Gründen für den Datenschutz.

[18] Für weitere Handlungsempfehlungen, wie eine Datenschutz-Folgenabschätzung durchzuführen ist, siehe z. B. die Website des PIAF-Projekts (Ein Privatsphäre-Folgenabschätzungsrahmen für den Datenschutz und die Rechte auf Privatsphäre) unter folgender Internetadresse: http://www.piafproject.eu/Index.html. PIAF ist ein von der Europäischen Kommission kofinanziertes Projekt, das die EU und ihre Mitgliedstaaten anregen will, eine fortschrittliche Privatsphäre-Folgenabschätzungspolitik als Gestaltungsmittel anzunehmen, um auf die Bedürfnisse und die Herausforderungen im Zusammenhang mit der Privatsphäre und der Verarbeitung personenbezogener Daten eingehen zu können. Auch in einigen Mitgliedstaaten stehen Handlungsempfehlungen zur Verfügung. Siehe beispielsweise das vom Datenschutzbeauftragten des Vereinigten Königreichs herausgegebene Handbuch für die Privatsphäre-Folgenabschätzung (privacy impact assessment (PIA) handbook) unter folgender Internetadresse: http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment; die von der französischen Datenschutzbehörde herausgegebenen Handlungsempfehlungen für die Risikoanalyse, auf die bereits oben in Fußnote 12 hingewiesen wurde, und die vom slowenischen Datenschutzbeauftragten vorgelegten Handlungsempfehlungen, die sich speziell mit 'Privatsphäre-Folgenabschätzungen in E-Government-Projekten' befasst und unter folgender Internetadresse abrufbar ist: https://webmail.europarl.europa.eu/exchweb/bin/redir.asp?URL=https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIASmernice__ENG_Lektorirano_10._6._2011.pdf

[19] Beispielsweise betreibt im Vereinigten Königreich ein Konsortium unter der Federführung der Universität Manchester und der Beteiligung der Universität Southampton, des Nationalen Statistikamtes und des neuen staatlichen Instituts für offene Daten (ODI) das Anonymisierungsnetz des Vereinigten Königreichs (UKAN), um damit den Austausch und die gemeinsame Nutzung von bewährten Verfahrensweisen im Zusammenhang mit der Anonymisierung im gesamten öffentlichen und privaten Sektor zu ermöglichen. Das Netz unterhält unter https://webmail.europarl.europa.eu/exchweb/bin/redir.asp?URL=http://www.ukanon.net eine Website und führt Fallstudien, Expertengutachten und Seminare durch.

5.1. Anwendbarkeit des allgemeinen Datenschutzrahmens auf die Weiterverwendung von Informationen des öffentlichen Sektors (PSI)

Nach dem Erwägungsgrund 21 der PSI-Richtlinie gilt Folgendes: "Diese Richtlinie sollte unter uneingeschränkter Beachtung der Grundsätze des Schutzes personenbezogener Daten […] durchgeführt und angewandt werden". Ferner gilt nach Artikel 1 Absatz 4: "Diese Richtlinie hat keinerlei Auswirkungen auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten […]".

5.2. Ausnahmen von den Gründen für den Schutz von personenbezogenen Daten

Diesbezüglich trifft die PSI-Richtlinie folgende Regelung: "Diese Richtlinie gilt nicht für […] Dokumente, die nach den Zugangsregelungen der Mitgliedstaaten nicht zugänglich sind […]"[20]

Ferner regelt die PSI-Richtlinie in der geänderten Fassung auch Ausnahmen aus Gründen des Datenschutzes. Artikel 1 Absatz 2 Buchstaben cc) regelt die folgenden drei Situationen, die alle von der Anwendung der PSI-Richtlinie ausgeschlossen sind:

- Dokumente, die nach den Zugangsregelungen der Mitgliedstaaten aus Gründen des Schutzes personenbezogener Daten nicht zugänglich sind;
- Dokumente, die nach den Zugangsregelungen der Mitgliedstaaten aus Gründen des Schutzes personenbezogener Daten nur eingeschränkt zugänglich sind; und
- 'Teile von Dokumenten, die nach diesen Regelungen zugänglich sind, wenn sie personenbezogene Daten enthalten, deren Weiterverwendung gesetzlich nicht mit dem Recht über den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten vereinbar ist'.

5.3. Allgemeine Bemerkungen

Die Datenschutzgruppe unterstreicht, dass die Weiterverwendung von Dokumenten für kommerzielle und nichtkommerzielle Zwecke gemäß den Bedingungen der PSI-Richtlinie ungeachtet des in der PSI-Änderungsrichtlinie formulierten 'Grundsatzes der Weiterverwendbarkeit' dann nicht immer angebracht ist, wenn die zur Weiterverwendung vorgesehenen Informationen des öffentlichen Sektors personenbezogene Daten enthalten. Die Entscheidungen betreffend die Weiterverwendung personenbezogener Daten gemäß den Bedingungen der PSI-Richtlinie müssen also auf der Grundlage der Beurteilung des Einzelfalls getroffen werden; außerdem ist es notwendig, zusätzliche rechtliche, technische und organisatorische Maßnahmen zum Schutz der betreffenden natürlichen Personen zu ergreifen.

Die Weiterverwendung von öffentlich zugänglichen personenbezogenen Daten ist eingeschränkt und sollte dies auch bleiben durch

- die allgemeinen Vorschriften des einschlägigen Datenschutzrechts,
- (gegebenenfalls) die zusätzlichen speziellen rechtlichen Einschränkungen und
- die technischen und organisatorischen Sicherheits- und Schutzmaßnahmen, die zum Schutz von personenbezogenen Daten ergriffen wurden.

[20] Siehe Artikel 1 Absatz 2Buchstabe c der PSI-Richtlinie.

5.4. Dokumente, die nicht zugänglich sind

Diese Bestimmung schließt vom Anwendungsbereich der PSI-Richtlinie alle Dokumente aus, die nach den Zugangsregelungen des betreffenden Mitgliedstaats aus Gründen des Schutzes personenbezogener Daten nicht zugänglich sind.

Anders als bei den Datenschutzgesetzen, die auf der Grundlage der Richtlinie 95/46/EG weitgehend harmonisiert sind, gibt es bei den Gesetzen über freien Informationszugang erhebliche Abweichungen unter den einzelnen Mitgliedstaaten der EU. Typischerweise schreiben die Zugangsregelungen eine Abwägungsprüfung vor, bei der die durch die Vorschriften zum Schutz der Privatsphäre und die Datenschutzvorschriften geschützten Interessen vergleichsweise den Vorteilen der Offenheit und der Transparenz gegenüberzustellen sind. Angesichts der vorhandenen rechtlichen Abweichungen kann das Ergebnis der Abwägungsprüfung in den verschiedenen Mitgliedstaaten der EU unterschiedlich ausfallen. Beispielsweise dürfen die Steuerbehörden in einigen Mitgliedstaaten bestimmte Teile der Einkommensteuererklärungen der Steuerzahler veröffentlichen (nach Maßgabe rechtlicher, technischer und organisatorischer Maßnahmen, um die Missbrauchsrisiken möglichst gering zu halten), wohingegen andere Mitgliedstaaten diese als Informationen einstufen würden, die unter die Ausnahmen fallen und daher generell vertraulich behandelt werden müssen.

Davon abgesehen müssen die nationalen Rechtsvorschriften mit Artikel 8 der Europäischen Menschenrechtskonvention ('EMRK') und mit den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union ('EU-Charta') im Einklang stehen. Dies bedeutet, wie der Europäische Gerichtshof in seinen Urteilen *Österreichischer Rundfunk* und *Schecke*[21] entschieden hat, dass erwiesen sein muss, dass die Offenlegung dem Zweck entsprechend notwendig ist und in einem angemessenen Verhältnis zu dem mit der nationalen Regelung verfolgten berechtigten Ziel steht.

In jedem Fall sind die in einem Dokument enthaltenen personenbezogenen Daten vom Anwendungsbereich der PSI-Richtlinie ausgeschlossen, wenn sie nach den Zugangsregelungen des betreffenden Mitgliedstaats nicht zugänglich sind (so auch für den Fall, dass die nationalen Rechtsvorschriften zu Transparenz und Offenheit keine Regelung zur allgemeinen Zugänglichkeit der betreffenden personenbezogenen Daten enthalten).

Um Rechtssicherheit und Transparenz gegenüber den betroffenen Personen zu gewährleisten, entspricht es guter Praxis, nach Möglichkeit einen proaktiven Ansatz zu verfolgen und im Voraus festzulegen, welche personenbezogenen Daten unter Umständen öffentlich zugänglich gemacht werden. Die betroffenen Personen können dann zum Zeitpunkt der Datenerhebung unterrichtet werden, ob etwa ein Teil der von ihnen mitgeteilten oder im Laufe des Verwaltungsverfahrens weiterzuverarbeitenden personenbezogenen Daten infolge der Gesetze über freien Informationszugang öffentlich zugänglich wird.

5.5. Dokumente, die nur eingeschränkt zugänglich sind

Diese Bestimmung schließt vom Anwendungsbereich der PSI-Richtlinie alle Dokumente aus, die nach den Zugangsregelungen des betreffenden Mitgliedstaats aus Gründen des Schutzes personenbezogener Daten nur eingeschränkt zugänglich sind. Auch hier können die Zugangsregelungen der verschiedenen Mitgliedstaaten Abweichungen in Bezug auf die Fragen

[21] Siehe Urteil des Gerichtshofes vom 20. Mai 2003, Österreichischer Rundfunk, Verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, und Urteil des Gerichtshofes vom 9. November 2010, Volker und Markus Schecke, Verbundene Rechtssachen C-92/09 und C-93/09.

aufweisen, welche Daten einem eingeschränkten Zugang unterliegen und welche Art von Zugangsbeschränkungen dort zum Tragen kommt. Dazu folgende Beispiele:

- Sammlungen von nationalen Archiven, die personenbezogene Daten enthalten, die nur nach Maßgabe spezieller Zugangsbedingungen und zusätzlicher Sicherheits- und Schutzmaßnahmen zugänglich sind (siehe Abschnitt IX weiter unten);
- Sammlungen von Forschungsdaten, die personenbezogene Daten enthalten, die nur nach Maßgabe spezieller Zugangsbedingungen und zusätzlicher Sicherheits- und Schutzmaßnahmen zugänglich sind (siehe Abschnitt VIII weiter unten);
- bestimmte Informationen in öffentlichen Registern, Gerichtsakten oder sonstigen Verwaltungsdokumenten, die personenbezogene Daten enthalten, die nur natürlichen Personen oder Organisationen mit einem berechtigten Interesse oder nur nach Maßgabe anderer spezieller Zugangsbedingungen und zusätzlicher Sicherheits- und Schutzmaßnahmen zugänglich sind.

5.6. Teile von zwar zugänglichen Dokumenten, deren Weiterverwendung aber unvereinbar ist

Diese Bestimmung schließt vom Anwendungsbereich der PSI-Richtlinie aus:

- Teile von Dokumenten,
- die nach nationalen Zugangsregelungen zugänglich sind,
- wenn sie personenbezogene Daten enthalten, deren Weiterverwendung gesetzlich nicht mit dem Recht über den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten vereinbar ist.

Diese Bestimmung bestätigt, dass auch wenn bestimmte Dokumente mit personenbezogenen Daten uneingeschränkt zugänglich sind, deren Weiterverwendung trotzdem aus Datenschutzgründen eingeschränkt sein kann.

Die Datenschutzgruppe betont, dass diese Bestimmung der PSI-Richtlinie im Lichte des Artikels 1 Absatz 4 der PSI-Richtlinie auszulegen ist, demzufolge gilt: „Diese Richtlinie hat keinerlei Auswirkungen auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten […]“.

Die Datenschutzgruppe würde es begrüßen, wenn in bewährter Verfahrensweise spezielle Rechtsvorschriften in nationales Recht aufgenommen würden, die eindeutig bestimmen, (i) welche Daten öffentlich zugänglich gemacht werden, (ii) zu welchen Zwecken dies erfolgt und gegebenenfalls (iii) in welchem Umfang und unter welchen Bedingungen deren Weiterverwendung gestattet ist. Solange solche speziellen Bestimmungen nicht in Kraft sind, bedeutet dies allerdings nicht, dass öffentlich zugängliche personenbezogene Daten im Rahmen der PSI-Richtlinie stets weiterverwendet werden dürfen.

Vielmehr bestimmt in diesen Fällen das Datenschutzrecht (in Verbindung mit anderen einschlägigen Rechtsvorschriften, wie z. B. den Bestimmungen über den Zugang zu Dokumenten), ob in dem konkreten Fall personenbezogene Daten zu Zwecken der Weiterverwendung zugänglich gemacht werden dürfen, und wenn ja, nach Maßgabe welcher zusätzlicher Sicherheits- und Schutzmaßnahmen. Ist das Ergebnis dieser Bewertung positiv, so wird die Weiterverwendung nach Maßgabe spezieller Datenschutzmaßnahmen und aller anderen in der PSI-Richtlinie festgelegten Bedingungen gestattet (solange das Datenschutzrecht nicht beeinträchtigt ist). Ist das Ergebnis dieser Bewertung negativ, so fällt eine Weiterverwendung nicht in den Anwendungsbereich der PSI-Richtlinie.

Die folgenden Beispiele dienen der Veranschaulichung, wann diese Ausnahme vom Anwendungsbereich der PSI-Richtlinie zutreffen kann. Im ersten Beispiel sind die Weiterverwendungsbeschränkungen eindeutig im Gesetz geregelt.

- Die Steuergesetze eines Mitgliedstaats können bestimmen, dass die Einkommensteuererklärungen aller Steuerinländer zwecks Überprüfung durch einen anderen Bürger auf Antrag in den Diensträumen der Steuerbehörden öffentlich zugänglich sind, ohne dass ein berechtigtes Interesse nachzuweisen ist. Im Gesetz ist ebenfalls eindeutig festgelegt, dass die Daten nicht in Verbindung mit anderen Daten weiterverarbeitet, so z. b. im Internet veröffentlicht, bzw. weiter redigiert werden dürfen. Eine NRO beantragt den Zugang zu diesen Daten und die Gestattung, die Steuererklärungsdatenbank weiterverwenden zu dürfen, um die Daten auf ihrer Website zu veröffentlichen. In diesem Fall befinden sich die Steuerdaten außerhalb des Anwendungsbereichs der PSI-Richtlinie und es besteht für die öffentliche Stelle keine Verpflichtung, den Datensatz zu Zwecken der Weiterverwendung im Rahmen der PSI-Richtlinie zugänglich zu machen.

In vielen anderen Fällen dürften die gesetzlichen Beschränkungen in Bezug auf die Weiterverwendung jedoch weniger klar und weniger kategorisch formuliert sein. Üblicherweise gestatten verschiedene Zivil-, Handels- und Einwohnermelderegister sowie sonstige Datenbanken eine Abfrage von personenbezogenen Daten durch die Öffentlichkeit, mehr und mehr auch in digitaler Form über das Internet. Häufig unterliegt die Zugriffsmöglichkeit speziellen Sicherheits- und Schutzmaßnahmen, einschließlich technischer Beschränkungen für Suchfunktionen und Massen-Downloads. Unter Umständen werden die Benutzer auch gebeten, gewissen Zugangsbedingungen zuzustimmen.

- Die Steuergesetze eines Mitgliedstaats können bestimmen, dass die Namen derjenigen Steuerpflichtigen, die über einen längeren Zeitraum Steuerrückstände über einem bestimmten Schwellenwert hatten, auf einer eigens dafür eingerichteten Internetseite für eine begrenzte Zeit veröffentlicht werden, und zwar nach Maßgabe zusätzlicher technischer Sicherheits- und Schutzmaßnahmen einschließlich technischer Beschränkungen für Suchfunktionen und Massen-Downloads. Mit dieser Veröffentlichung sollen die Steuerpflichtigen zur rechtzeitigen Zahlung der Einkommenssteuer angehalten und denjenigen, die dies nicht tun, zusätzlich eine (ihren guten Ruf belastende) Art von Bestrafung erteilt werden. Ein Bankenkonsortium beantragt zu Zwecken der Weiterverwendung Zugang zu den Daten, um diese in sein Kreditauskunftei-System einzuspeisen.
- Spezialgesetze im Gesundheitswesen eines Mitgliedstaates können den Patienten nach Maßgabe von Sicherheits- und Schutzmaßnahmen gestatten, auf einer eigens dafür eingerichteten Internetseite zu überprüfen, ob einem bestimmten Arzt oder sonstigen Angehörigen der Heilberufe das Praktizieren untersagt wurde. Dabei kommen technische Sicherheits- und Schutzmaßnahmen einschließlich technischer Beschränkungen für Suchfunktionen und Massen-Downloads zur Anwendung. Eine Patientenrechtsorganisation beantragt zu Zwecken der Weiterverwendung Zugang zu den Daten, um eine mehrsprachige und benutzerfreundlichere Website für den Zugriff auf diese Daten einzurichten.
- Spezialgesetze eines Mitgliedstaates können die Veröffentlichung der Namen der Geber vorschreiben, die einer politischen Partei eine Spende über einem bestimmten Schwellenwert gegeben haben. Diese Information, die Aufschluss über die politische Einstellung der Geber geben kann, wird auf einer eigens dafür eingerichteten Website öffentlich gemacht. Dabei kommen technische Sicherheits- und Schutzmaßnahmen einschließlich technischer Beschränkungen für Suchfunktionen und Massen-Downloads zur Anwendung. Eine Aktivistengruppe beantragt zu Zwecken der Weiterverwendung im Rahmen der PSI-

Richtlinie Zugang zu den Daten im Ganzen, um eine neue Website mit zusätzlichen Funktionen und besseren Suchmöglichkeiten einzurichten.

- Name und Anschrift des Eigentümers einer Immobilie sind zwar im Grundbuch des betreffenden Mitgliedstaates öffentlich verzeichnet, aber das Surfen in der öffentlich zugänglichen Datenbank ist so eingeschränkt, dass nur die Suche nach einer bestimmten Immobilie und eben nicht die Suche nach einer bestimmten natürlichen Person möglich ist. Auch Massen-Downloads sind begrenzt. Ein gewerbliches Unternehmen beantragt zu Zwecken der Weiterverwendung Zugang zu den Daten im Ganzen, um eine benutzerfreundlichere Website zu einem konkurrenzfähigeren Preis einzurichten.
- Das Handelsregister eines Mitgliedstaates gestattet den öffentlichen Zugang zu einer breiten Palette personenbezogener Daten, so zu Namen, Anschriften und Unterschriftsproben der Unternehmensvorstände/Geschäftsführer und zu Informationen über die Eigentumsverhältnisse bei bestimmten Unternehmenstypen. Es bestehen einige Beschränkungen für Suchfunktionen und für die Anzahl der Posten, die heruntergeladen werden können. Die Informationen sind über eine eigens dafür eingerichtete Internetseite gegen Gebühr abrufbar. Ein gewerbliches Unternehmen beantragt zu Zwecken der Weiterverwendung Zugang zu den Daten im Ganzen, um eine Website einzurichten, die die Informationen aus mehreren verschiedenen Registern miteinander kombiniert und damit verbesserte Informationen zu einem konkurrenzfähigeren Preis anzubieten hat.

In allen Fällen muss die betreffende öffentliche Stelle eine sorgfältige Datenschutz-Folgenabschätzung vornehmen, anhand deren sie entscheiden kann, ob die betreffenden Daten zu Zwecken der Weiterverwendung im Rahmen der PSI-Richtlinie zugänglich gemacht werden dürfen, und wenn ja, ob nach dem einschlägigen Datenschutzrecht spezielle Bedingungen und Schutzmaßnahmen vorgeschrieben sind. Der ‘Grundsatz der Weiterverwendbarkeit’ setzt keinen Automatismus frei und vermag die einschlägigen Bestimmungen des Datenschutzrechts nicht auszuhebeln.

Diese sorgfältige Folgenabschätzung ist umso wichtiger, als die betreffende öffentliche Stelle im Rahmen der PSI-Richtlinie im Grunde nicht berücksichtigen muss, um wen es sich bei dem speziellen Wiederverwender, der Zugang zu den Daten beantragt hat, handelt. Nach Artikel 10 (Nichtdiskriminierung) gilt: “Die Bedingungen für die Weiterverwendung von Dokumenten sind für vergleichbare Kategorien der Weiterverwendung nichtdiskriminierend“. Ferner bestimmt Artikel 11 (Verbot von Ausschließlichkeitsvereinbarungen): “Die Weiterverwendung von Dokumenten steht allen potenziellen Marktteilnehmern offen […]. Verträge oder sonstige Vereinbarungen zwischen den öffentlichen Stellen, die im Besitz der Dokumente sind, und Dritten dürfen keine ausschließlichen Rechte gewähren“.

Daher müssen die öffentlichen Stellen bei der Entscheidung, ob die Weiterverwendung gestattet werden soll, auch berücksichtigen, ob die Gestattung der Weiterverwendung im Rahmen einer offenen Lizenz, die nicht nur für den Antragsteller, sondern für jedermann gilt, der die Daten anfordert, mit dem Datenschutzrecht vereinbar ist. Dies verlangt ein hohes Maß an Vertrauen, dass keiner der potenziellen Weiterverwender in der Lage sein wird, die bereitgestellten personenbezogenen Daten missbräuchlich zu verwenden.

Nach der PSI-Richtlinie ist nicht ausgeschlossen, dass die Weiterverarbeitung nach Maßgabe der Bedingungen etwa nur zu bestimmten Zwecken gestattet wird. Für die öffentliche Stelle stellt sich dann die Frage, ob die Weiterverwendung zu diesen Zwecken durch jeglichen ‘potenziellen Marktteilnehmer’ mit den von der öffentlichen Stelle festgelegten Zwecken im Einklang steht. Die potenzielle Weiterverwendung der Informationen über die Zahlungsweise der Einkommenssteuer

durch Finanzinstitute, so z. B. zu Zwecken der Kreditauskunft, hat Relevanz, da diese nach der Prüfung des Begriffs ‘eine andere Person’ weiterhin ein potenzieller Weiterverwender sind. Um den Belangen des Datenschutzes gerecht zu werden und insbesondere sicherzustellen, dass der Grundsatz der Zweckbindung eingehalten wird, muss es der öffentlichen Stelle (bzw. dem Gesetzgeber) daher erlaubt sein, den Zweck der Weiterverwendung gegebenenfalls einzuschränken.

VI. Weiterverwendung von aggregierten und anonymisierten Datensätzen, die von personenbezogenen Daten abgeleitet wurden

6.1. Welche Vorteile bieten Aggregation und Anonymisierung für die Zwecke der Weiterverwendung von Informationen des öffentlichen Sektors (PSI)?

Bisher zielten die von öffentlichen Stellen im Rahmen von ‘Open-Data-Portalen’ oder sonstigen Plattformen angestoßenen Initiativen für die Weiterverwendung von Informationen des öffentlichen Sektors typischerweise darauf ab, eher aggregierte und anonymisierte als echte personenbezogene Daten für die Weiterverwendung bereitzustellen. Dieser Ansatz verspricht tatsächlich mehr Sicherheit und sollte gefördert werden.

Die Datenschutzgesetze gestatten es in der Regel nicht, dass öffentliche Stellen personenbezogene Daten, die für einen anderen, für gewöhnlich einen administrativen Zweck erhoben wurden, offenlegen[22]. Daher ist in diesen Fällen ihre Weiterverwendung als Bestandteil von Initiativen für die Weiterverwendung von Informationen des öffentlichen Sektors auch nicht möglich. Statt personenbezogenen Daten sind es üblicherweise statistische Daten, die aus personenbezogenen Daten abgeleitet wurden, die zu Zwecken der Weiterverwendung bereitgestellt werden und – auch vom Grundsatz her – bereitgestellt werden sollten. Dies ist die effektivste Lösung, um das Risiko einer versehentlichen Offenlegung personenbezogener Daten möglichst gering zu halten. Diese anonymisierten und aggregierten Datensätze sollten es unmöglich machen, dass natürliche Personen rückidentifiziert und wiedererkannt werden können, und sollten daher keinerlei personenbezogene Daten enthalten.

Bei der Entscheidung, welches Aggregationsniveau angemessen ist und welche speziellen Anonymisierungstechniken zur Anwendung kommen sollen, handelt es sich um eine anspruchsvolle Aufgabe. Werden nämlich Aggregation und Anonymisierung nicht effektiv gehandhabt, so birgt dies das Risiko, dass sich die betreffenden natürlichen Personen gleichwohl aus diesen Datensätzen wiedererkennen lassen. Daher hat das Datenschutzrecht bei der Festlegung der Schwelle, bei der es ‘sicher’ ist, anonymisierte und aggregierte Daten als Bestandteil einer PSI-Initiative freizugeben, eine bedeutende Rolle zu spielen.

Die Richtlinie 95/46/EG legt eine hohe Schwelle für die Anonymisierung fest

Die Verwendung des Begriffs 'Anonymisierung' in diesem Dokument bezieht sich auf Daten, die nicht mehr als personenbezogene Daten im Sinne des Artikels 2 Buchstabe a der Richtlinie 95/46/EG gelten können. Artikel 2 Buchstabe a definiert 'personenbezogene Daten' als 'alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“); als bestimmbar wird eine Person angesehen, die direkt oder indirekt rückidentifiziert werden kann, insbesondere durch Zuordnung einer Kennnummer oder zu einem oder mehreren spezifischen

[22] Natürlich können die Rechtsvorschriften über die Informationsfreiheit gegebenenfalls die Offenlegung von personenbezogenen Daten erforderlich machen und das Interesse an Transparenz und an der Verfügbarkeit von Information in gewissen Situationen die Belange des Datenschutzes und der Privatsphäre aus den Angeln heben. Denn es handelt sich hierbei um ein sich weiterentwickelndes Rechtsgebiet, das in Zukunft Veränderungen mit sich bringen dürfte.

Elementen, die Ausdruck ihrer physischen, psychologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind'.[23]

Ebenfalls relevant ist der Erwägungsgrund 26 der Richtlinie 95/46/EG, der folgende Feststellung trifft: 'Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen'.

Es muss betont werden, dass dies eine hohe Schwelle festlegt, wie in dieser Stellungnahme noch weiter erörtert wird. Sofern die Daten nicht anonymisiert werden können, um diese Schwelle zu erreichen, findet das Datenschutzrecht nach wie vor Anwendung. Dies bedeutet unter anderem, dass sofern die Schwelle nicht erreicht wird, die öffentliche Freigabe der Informationen (und jede weitere Nutzung) mit den ursprünglichen Zwecken der Erhebung der Daten im Sinne des Artikels 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG 'vereinbar' sein muss. Ferner muss für die Verarbeitung im Rahmen des Artikels 7 Buchstaben a bis f der Richtlinie 95/46/EG auch ein angemessener Rechtsgrund bestehen (so z. B. Zustimmung oder die Notwendigkeit, die gesetzlichen Vorschriften zu erfüllen). Wurden die Daten hingegen im Sinne des Artikels 2 Buchstabe a und des Erwägungsgrundes 26 der Richtlinie 95/46/EG anonymisiert, so finden die Datenschutzvorschriften keine Anwendung mehr und die Weiterverwender dürfen die Daten ohne diese Zwänge weiterverwenden.

Es muss noch einmal betont werden, dass der Begriff 'anonymisierte Daten', wie er in dieser Stellungnahme verwendet werden, sich auf Daten bezieht, die nicht mehr als personenbezogene Daten gelten. Anonymisierte Daten sind insbesondere von Daten zu unterscheiden, die mithilfe verschiedener Techniken manipuliert wurden, um das Risiko der Identifizierung/Wiedererkennung der betreffenden natürlichen Personen zu entschärfen, die aber die nach Artikel 2 Buchstabe a und Erwägungsgrund 26 der Richtlinie 95/46/EG erforderliche Schwelle nicht erreicht haben.[24] In vielen Szenarios eignen sich diese Techniken nur für eine eingeschränkte Offenlegung zu Zwecken der Weiterverwendung durch überprüfte Dritte, nicht aber für die vollständige Offenlegung und Weiterverwendung im Rahmen einer offenen Lizenz.

Es muss auch betont werden, dass, sobald die Daten zu Zwecken der Weiterverwendung öffentlich freigegeben wurden, nicht mehr zu kontrollieren ist, wer Zugriff auf die Daten hat. Die Wahrscheinlichkeit, dass 'eine andere Person' über die Mittel verfügt und diese Mittel auch einsetzt, um die betroffenen Personen zu identifizieren, wird ganz erheblich zunehmen. Wenn es dazu kommt, Daten zu Zwecken der Weiterverwendung im Rahmen der PSI-Richtlinie bereitzustellen, möchte die Artikel-29-Datenschutzgruppe unbeschadet der Auslegung des Erwägungsgrundes 26 in anderen Zusammenhängen daher eindeutig klarstellen, dass äußerste Sorgfalt angebracht ist, um sicherzustellen, dass die offenzulegenden Datensätze keinerlei Daten beinhalten, die sich mit Mitteln identifizieren und wiedererkennen lassen, die ziemlich wahrscheinlich auch von einer anderen Person, einschließlich potenzieller Weiterverwender, aber auch von anderen Parteien, die ein

[23] In ihrer (weiteren) Stellungnahme vom 27. Februar 2013 zu 'den derzeitigen Diskussionen um das Datenschutz-Reformpaket' betonte die Datenschutzgruppe, dass 'eine natürliche Person als bestimmbar anzusehen ist, wenn sie innerhalb einer Personengruppe von anderen Personen unterschieden und folglich unterschiedlich behandelt werden kann. Dies bedeutet, dass der Begriff der Bestimmbarkeit die Aussonderung mit beinhaltet'. Die Stellungnahme stellt auch klar, dass 'Identifikationsnummern, Standortdaten, IP-Adressen, Online-Kennungen oder sonstige spezifische Faktoren in Bezug auf eine natürliche Person als personenbezogene Daten anzusehen sind'.

[24] In der (weiteren) Stellungnahme vom 27. Februar 2013 wird betont, dass 'wenn es möglich ist, eine natürliche Person zurückzuverfolgen oder eine natürliche Person mit anderen Mitteln (indirekt) zu identifizieren, die Datenschutzbestimmungen weiterhin Anwendung finden.'

Interesse an diesen Daten haben können, so auch von den Strafverfolgungsbehörden, eingesetzt werden.

Weitere Orientierungshilfen zur Anonymisierung und zum Begriff personenbezogene Daten

Für weitere Orientierungshilfen zur Anonymisierung und zum Begriff personenbezogene Daten, siehe die Stellungnahme 4/2007 der Datenschutzgruppe zum Begriff personenbezogene Daten, angenommen am 20. Juni 2007 (WP 136). Die Datenschutzgruppe kann im zweiten Halbjahr 2013 auch noch weitere Orientierungshilfen in einem eigenen Dokument zu den Anonymisierungstechniken geben.

6.2. Welche Herausforderungen und Grenzen bestehen für die Anonymisierung zu Zwecken der Weiterverwendung von Informationen des öffentlichen Sektors (PSI)?

Angesichts der Fortschritte der modernen Computertechnologie und der allgegenwärtigen Verfügbarkeit von Informationen ist die Anonymisierung immer schwerer zu bewerkstelligen. Die Rückidentifizierbarkeit von natürlichen Personen gerät immer mehr zu einer allgemeinen und gegenwärtigen Gefahr.[25] Praktisch gibt es eine sehr beträchtliche Grauzone, bei der ein für die Verarbeitung der Daten Verantwortlicher bei der Freigabe der Daten etwa glaubt, dass ein Datensatz anonymisiert ist, ein Dritter aber immer noch in der Lage ist, wenigstens ein paar natürliche Personen aus den Daten zu identifizieren, so z. B. mithilfe anderer öffentlich zugänglicher Informationen bzw. mithilfe anderer ihm zur Verfügung stehender Informationen.

Einer der größten Risikofaktoren ist die anwachsende Menge an Online- und Offlinedaten, die sowohl öffentlich zugänglich als auch in den Händen von Wirtschaftsorganisationen konzentriert sind und dann zur Erstellung des Persönlichkeitsprofils natürlicher Personen zu Zwecken der verhaltensgesteuerten Internetwerbung und für ein weiter wachsendes Spektrum an anderen Zwecke genutzt werden kann. Gemessen an der Realität der 'großen Daten', die diesen Organisationen bereits zur Verfügung stehen, dürften die aus personenbezogenen Daten abgeleiteten und zu Zwecken der Weiterverwendung bereitgestellten Informationen des öffentlichen Sektors die Wahrscheinlichkeit erhöhen, dass natürliche Personen jetzt rückidentifiziert werden könnten oder dass ihre Profile weiter angereichert werden, oftmals ohne dass die betreffenden Personen sich dessen bewusst sind, was gerade mit ihnen geschieht.

6.3. Wer soll die Aggregation und die Anonymisierung durchführen und wann?

Die Aggregation und die Anonymisierung sollten zum frühesten möglichen Zeitpunkt durchgeführt werden, und zwar von dem für die Verarbeitung Verantwortlichen oder einem vertrauenswürdigen Dritten im Namen des für die Verarbeitung Verantwortlichen bzw. mehrerer Verantwortlicher

[25] Siehe beispielsweise 'Transparent Government, Not transparent Citizens' (Transparente Regierung, nicht transparente Bürger), ein Bericht für das UK Cabinet office, 2011 vorgelegt von Kieron O'Hara, Southampton University, in dem der Autor vor der Fähigkeit warnte, natürliche Personen aus anonymisierten Daten mithilfe u. a. von 'Puzzle-Identifizierung' wiedererkennbar zu machen, und dazu feststellt, dass es keine vollkommenen technischen Lösungen für das Entanonymisierungsproblem gibt. Der Bericht ist über Internet abrufbar unter: http://www.cabinetoffice.gov.uk/sites/default/files/resources/transparency-and-privacy-review-annex-b.pdf.Siehe auch 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (Gebrochene Versprechen zur Privatsphäre: Antworten auf die überraschenden Misserfolge bei der Anonymisierung), vorgelegt von Paul Ohm, University of Colorado Law School, 57 UCLA Law Review 1701 (2010), über Internet abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

(der/die auch über die notwendigen Spezialkenntnisse verfügt/verfügen). Es kann nicht dem Weiterverwender überlassen bleiben, die Anonymisierung durchzuführen, so z. B. als Bedingung für die Lizenzerteilung. Ferner ist unbedingt sicherzustellen, dass die etwaige Anbieterorganisation, die als Dritter die Aggregation und die Anonymisierung durchführt, in keinem Interessenkonflikt steht und eindeutig in die Verantwortung genommen wird, dass die personenbezogenen Daten nur dazu verwendet werden, diese Anonymisierung durchzuführen, und dass zu diesem Zweck alle erforderlichen Sicherungs- und Schutzmaßnahmen ergriffen werden. Die Drittorganisation muss ebenso garantieren können, dass die personenbezogenen Daten, aus denen die aggregierten und anonymisierten Datensätze abgeleitet werden, gelöscht werden, sobald sie zu diesem Zweck nicht mehr benötigt werden.

6.4. Bewertung des Risikos der Rückidentifizierung

Sofern die Daten nicht im Sinne des Artikels 2 Buchstabe a und des Erwägungsgrundes 26 der Richtlinie 95/46/EG anonymisiert werden können, findet das Datenschutzrecht weiter Anwendung.

Die für die Verarbeitung Verantwortlichen haben nach den Regeln der Vernunft zu bewerten, ob eine natürliche Person aus dem ‘anonymisierten’ Datensatz, der zu Zwecken der Weiterverwendung bereitgestellt werden soll, sowie aus anderen Daten identifiziert werden kann. Mit anderen Worten, ob eine Organisation oder eine natürliche Person aus den Daten, die freigegeben werden, eine andere natürliche Person wiedererkennen kann, und zwar entweder aus den freigegebenen Daten selbst oder in Kombination mit anderen verfügbaren Informationen.

Wie bereits in Abschnitt 6.1 erläutert wurde, zielt diese Stellungnahme nicht darauf ab, umfassende und abschließende Handlungsempfehlungen zu geben, wie die Risiken der Rückidentifizierung zu bewerten sind. Sie stellt auch nicht darauf ab, eine abschließende Definition für 'Anonymisierung' bzw. 'anonymisierte Daten' zu bieten. Sie weist jedoch wiederholt darauf hin, dass der Leser weitere Handlungsempfehlungen in den vorhandenen Dokumenten finden kann (so auch in den in Abschnitt 6.1 genannten Dokumenten), und dass in der Untergruppe 'Technologie' der Datenschutzgruppe auch noch Arbeiten über Anonymisierungstechniken im Gange sind, wie in den Abschnitten 6.1 und 2.2. bereits angemerkt wurde.

Vor diesem Hintergrund möchte die Artikel-29-Datenschutzgruppe ohne Anspruch auf Vollständigkeit noch einige Faktoren/Überlegungen hervorheben, die bei der Bewertung der Risiken einer Rückidentifizierung hilfreich sind, so insbesondere

- die Fragen, welche sonstigen Daten entweder für die allgemeine Öffentlichkeit oder für andere natürliche Personen oder Organisationen verfügbar sind, und ob die Daten, die veröffentlicht werden sollen, mit anderen Datensätzen verknüpft werden können;
- die Wahrscheinlichkeit, dass der Versuch einer Rückidentifizierung unternommen wird (einige Datenarten sind für potenzielle Eindringlinge attraktiver als andere); und
- die Wahrscheinlichkeit, dass die Rückidentifizierung, wenn denn ein Versuch unternommen wird, unter Berücksichtigung der Effektivität der vorgeschlagenen Anonymisierungstechniken[26] erfolgreich ist.

[26] Zu den Anonymisierungstechniken vgl. die kommende Stellungnahme der Artikel-29-Datenschutzgruppe zu diesem speziellen Thema.

Welche ‘sonstigen’ Informationen gibt es noch?

Bei der Ermittlung, ob eine natürliche Person indirekt rückidentifiziert werden kann, ist zu prüfen, ob die Rückidentifizierung anhand der fraglichen Daten möglich ist (in unserem Fall also anhand des 'anonymisierten' Datensatzes), oder etwa anhand dieser Daten zusammen mit *noch weiteren Informationen*, die sich im Besitz der Organisation bzw. der natürlichen Person, die den Rückidentifizierungsversuch unternimmt, bereits befinden oder eventuell/wahrscheinlich noch in deren Besitz kommen.

Bei diesen ‘weiteren Informationen’, die zu einer erfolgreichen Durchführung der Rückidentifizierung nötig sind, kann es sich um Informationen handeln, die bestimmten Unternehmen oder sonstigen Organisationen einschließlich der Strafverfolgungsbehörden und anderer öffentlicher Einrichtungen, bestimmten natürlichen Personen oder auch jedermann zugänglich sind, weil sie z. B. im Internet veröffentlicht wurden. Ein offensichtliches Beispiel dafür wäre, wenn öffentlich zugängliche Daten – wie z. B. das Wählerverzeichnis, das Telefonbuch oder andere bei einer Internetrecherche leicht auffindbare Daten – sich mit den (ungenügend) ‘anonymisierten’ Daten so kombinieren lassen, dass eine natürliche Person daraus identifiziert werden kann (z. B. mithilfe der Eingabe ihres Geburtsdatums und der Postleitzahl ihres Wohnortes).

Das Risiko der Rückidentifizierung kann sich erhöhen, wenn eine natürliche Person oder eine Gruppe von natürlichen Personen bereits eine Menge über eine andere natürliche Person weiß, z. B. ein Familienmitglied, einen Arbeitskollegen, einen Kontakt in einem sozialen Netz, einen Arzt, Lehrer, Vollzugsbeamten oder anderweitigen Angehörigen einer bestimmten Berufsgruppe kennt.

Worauf es hier jedoch ankommt, ist nicht etwa, ob die natürliche Person mit den entsprechenden Vorkenntnissen die jeweilige betroffene Person rückidentifizieren kann, sondern vielmehr, ob sie etwas Neues aus den durch die Identifizierung gewonnenen Informationen lernen wird. Die beiden nachstehend angeführten Beispiele veranschaulichen, wie wichtig diese Unterscheidung ist.

Beispiel 1: Masern-Statistik. Im einen Fall können anonymisierte statistische Daten offenlegen, dass sich in der Stadt A im Jahr 2012 X-Leute mit Masern angesteckt haben. Es erfolgt keine nähere Aufschlüsselung oder eingehendere Information. Ein Arzt, der Daten zu dieser Statistik beitrug, indem er den zuständigen Gesundheitsbehörden Angaben zu seinen eigenen Patienten machte, hat in seiner Praxis noch vollständigere Aufzeichnungen über diese Patienten, die aber der ärztlichen Schweigepflicht unterliegen. Der Arzt wäre also in der Lage, ohne Schwierigkeiten bei mehreren der Patienten aus dem statistischen Datensatz eine Rückidentifizierung vorzunehmen. Ganz ähnlich könnte eine Mutter, die weiß, dass ihr Kind sich in diesem Jahr mit Masern infizierte, ihr Kind ohne Schwierigkeiten im Datensatz wiedererkennen. Jedoch lernen weder die Mutter noch der Arzt etwas Neues aus dem anonymisierten und öffentlich zugänglich gemachten Datensatz, was sie zuvor noch nicht wussten.

Beispiel 2: Drogen- und Alkoholmissbrauch, sexueller Missbrauch sowie schulische Leistungen. Dieses Beispiel kann dem nachfolgenden Beispiel vergleichend gegenübergestellt werden. Es werden Forschungsarbeiten durchgeführt, die sich mit den Zusammenhängen und Wechselbeziehungen zwischen dem Drogen- und Alkoholmissbrauch der Eltern, dem sexuellen Missbrauch der Kinder und deren schulischen Leistungen befassen. Daraus werden mit guten Absichten vermeintlich 'anonymisierte' Forschungsdaten veröffentlicht, bei denen allerdings keine sorgfältige Bewertung der Identifikations-/Wiedererkennungsrisiken vorgenommen wurde.

Die statistischen Daten offenbaren unter anderem, dass in der Schule A, an der insgesamt 500 Schüler eingeschrieben sind, im Jahr 2012 20 % der Schüler (100 Schüler) in einem Haushalt lebten,

in dem zumindest ein Elternteil Alkoholiker oder Drogenabhängiger ist. Von diesen 100 Schülern wurde in 8 % der Fälle (8 Schüler) das Kind sexuell missbraucht. Der Forschungsbericht präzisiert zudem, dass an der Schule A keine weiteren Schüler sexuell missbraucht wurden.

Die Zahlen zeigen auch, dass in 96 % der Fälle (96 Schüler) die Kinder, deren Eltern alkohol- oder drogenabhängig sind, mit ihren schulischen Leistungen erheblich ins Hintertreffen gerieten (‘Schüler mit schwachen Leistungen’ nach der Definition eines angemessenen Bildungsstandards), dass an dieser speziellen Schule jedoch nur 50 % der sexuell missbrauchten Schüler (4 Schüler) erhebliche Schwierigkeiten mit den Schularbeiten hatten.

An dieser Schule ist allgemein bekannt, dass AA, ein intelligenter und hart arbeitender Junge, einen schwierigen familiären Hintergrund hat und seine Mutter Alkoholikerin ist. Er wird von seinen Klassenkameraden häufig schikaniert. Dieselben Klassenkameraden entdecken jetzt aus den in der Schulzeitung neu veröffentlichten statistischen Daten, dass AA unter die 50 % der sexuell missbrauchten Kinder fallen muss, die keine schulischen Schwierigkeiten haben (‘Schüler mit guten Leistungen’). Somit haben sie aus einem ineffektiv anonymisierten Datensatz neue (und in diesem Fall sehr sensible) Informationen dazugelernt.

Das Risiko, dass Informationen miteinander kombiniert werden, um daraus personenbezogene Daten zu schaffen, nimmt zu, da sich die Datenverknüpfungstechniken und die Rechenleistungen weiterentwickeln und immer mehr potenziell ‘miteinander kombinierbare’ Informationen öffentlich zugänglich werden. Denn die Rechenleistung verdoppelt sich jedes Jahr, und die Datenspeicherung dürfte wegen des großen Angebots an Cloud-Dienstleistungen zum Verbrauchsgut werden. Insofern ist das Risiko der Rückidentifizierung/Wiedererkennung mittels Datenverknüpfung unkalkulierbar, weil sich nie mit Gewissheit bewerten lässt, welche Daten schon zugänglich sind und welche Daten vielleicht künftig freigegeben werden.

Trotz aller Ungewissheiten lassen sich die Rückidentifizierungsrisiken für gewöhnlich zumindest in gewissem Maße abschwächen, indem man den Grundsatz der Datensparsamkeit befolgt, d. h. sicherstellt, dass nur die für einen bestimmten Zweck notwendigen Daten freigegeben werden.

Bei Wahrscheinlichkeit, dass der Versuch der Rückidentifizierung erfolgreich ist: „Test über den ‘motivierten Eindringling’“

Bei dem „Test über den ‘motivierten Eindringling’“ handelt es sich um ein innovatives Konzept, das noch voll auszutesten ist. Es kann hilfreich sein, zu ermitteln,

- ob jemand motiviert sein könnte, eine Rückidentifizierung vorzunehmen, und
- ob diese Rückidentifizierung eventuell/wahrscheinlich erfolgreich ist.

Der „Test über den ‘motivierten Eindringling’“ umfasst im Wesentlichen eine Prüfung, ob ein ‘Eindringling’ in der Lage wäre, eine Rückidentifizierung zu bewerkstelligen, *wenn* er genügend motiviert ist, dies einmal zu versuchen. Der ‘motivierte Eindringling’ ist jemand (eine natürliche Person oder eine Organisation), der den Wunsch hat, eine natürliche Person zu identifizieren, von deren personenbezogenen Daten anonymisierte Daten abgeleitet wurden. Der Test ist auf die Bewertung ausgerichtet, ob der motivierte Eindringling Erfolg haben könnte. Vom Konzept her geht er davon aus, dass der ‘motivierte Eindringling’ kompetent ist und auf Ressourcen zugreifen kann, die seiner vermutlichen Motivation zur Rückidentifizierung entsprechend groß sind.

Einige Arten von Daten dürften für einen ‘motivierten Eindringling’ attraktiver als andere Datenarten sein. So dürfte ein Eindringling beispielsweise im Allgemeinen höher motiviert sein, bestimmte personenbezogene Daten zurück zu identifizieren, wenn diese Daten

- einen erheblichen kommerziellen Wert haben (auch auf dem Schwarzmarkt oder außerhalb der Europäischen Union) und somit zu Zwecken des finanziellen Gewinns gekauft und verkauft werden können[27];
- zu Zwecken der Rechtsdurchsetzung/Vollstreckung oder zu Aufklärungszwecken eingesetzt werden können;
- berichtenswerte Neuigkeiten über Personen des öffentlichen Lebens aufdecken können;
- für politische oder aktivistische Zwecke (z. B. als Bestandteil einer Kampagne gegen eine spezielle Organisation oder Person) eingesetzt werden können;
- aus böswilligen persönlichen Gründen (z. B. Stalking, Belästigung, Schikane oder nur um andere in Verlegenheit zu bringen) instrumentalisiert werden können;
- Neugierde wecken können (z. B. das Verlangen einer ortskundigen Person, herauszufinden, wer in einen Vorfall verwickelt war, der auf einer Kriminalitätskarte verzeichnet ist).

Zwar ist es hilfreich, in den Bahnen der potenziellen Motivation des potenziellen Eindringlings zu denken, doch möchte die die Artikel-29-Datenschutzgruppe betonen, dass es für dieses Konzept auch beachtliche Grenzen gibt:

- Das Vorhaben kann in gewissem Maße spekulativ sein.
- Ohne offensichtlich 'motivierende Faktoren', wie den weiter oben beschriebenen, kann das Vorhaben zu trügerischen Sicherheitsgefühlen führen, die nahelegen, dass personenbezogene Daten, die relativ harmlos sind, zu Zwecken der Weiterverwendung ohne eine effektive Anonymisierung zugänglich gemacht werden können.
- Eindringlinge können raffiniert, innovativ und 'stets einen Schritt voraus sein' und Anwendungen für anonymisierte Daten finden, die für andere nicht unbedingt auf der Hand liegen.
- Mit den wachsenden Tendenzen zur 'Big-Data'-Analytik besteht auch ein immer höheres Risiko, dass erst einmal anonymisierte, scheinbar harmlose Daten, letztendlich noch viel ernstere Risiken darstellen können, sobald sie mit anderen Informationen kombiniert werden.

6.5. Testen der Rückidentifizierung

Unter gewissen Umständen kann es schwierig sein, das Rückidentifizierungsrisiko festzustellen, so insbesondere, wenn von einem Dritten unter Umständen komplizierte Statistikmethoden verwendet werden, um verschiedene Teile anonymisierter Daten zusammenzufügen. Als Teil der Gesamtbewertung zur Feststellung des Rückidentifizierungsrisikos ist es daher bewährte Praxis, den Rückidentifizierungstest durchzuführen – eine Art ‘Penetrationstest’ oder ‘Pentest’ – um die Schwachstellen einer Rückidentifizierung ausfindig zu machen und zu beheben. Dabei handelt es

[27] Dazu können z. B. gehören: Transaktions- oder sonstige Verhaltensdaten, aus denen sich individuelle Verbraucherprofile ableiten lassen, die dann zu Werbezwecken oder zu Zwecken der Preisdifferenzierung genutzt werden; Finanzinformationen oder sonstige Informationen, die einen Identitätsdiebstahl möglich machen; sensible Informationen, die zur Erpressung von natürlichen Personen oder zu ihrer Diskriminierung benutzt werden können; medizinische Daten, die von den Krankenversicherungsgesellschaften herangezogen werden können, so z. B. um den Krankenversicherungsschutz aufgrund einer vorhandenen Vorerkrankung zu versagen; Informationen, die Rückschlüsse auf die Kreditwürdigkeit erlauben und zur Bewertung von Kreditausfallrisiken herangezogen werden können, usw.

sich um den Versuch, natürliche Personen aus den Datensätzen, die freigegeben werden sollen, zurück zu identifizieren.

Die erste Phase eines Rückidentifizierungs-Testverfahrens besteht darin, die Datensätze bestandsmäßig zu erfassen, die die öffentliche Stelle veröffentlicht hat bzw. veröffentlichen will. In der nächsten Phase geht es darum, zu ermitteln, welche anderen Daten – personenbezogene und sonstige Daten – verfügbar sind, um sie mit den Daten zu verknüpfen, die in die Rückidentifizierung münden sollen. Insbesondere zielgerichtete 'Penetrationstests' sollten bei der Bewertung helfen, welches die Risiken der Puzzle-Identifizierung sind, d. h. des Zusammensetzens von verschiedenen Informationsteilchen, um ein vollständigeres Bild von jemandem zu schaffen.

Natürlich darf der Rückidentifizierungstest nicht als Patentrezept angesehen werden und ein trügerisches Sicherheitsgefühl bewirken. Erstens könnte sich der Test als schwierig durchzuführen erweisen, da er oftmals erhebliches technisches Fachwissen und angemessene Instrumente sowie die Kenntnis verlangt, welche anderen Daten zur Verfügung stehen. Zweitens müssen sich die für die Verarbeitung Verantwortlichen der Tatsache bewusst sein, dass sich das Risiko einer Rückidentifizierung im Laufe der Zeit ändern kann. Beispielsweise stehen jetzt immer stärkere und erschwinglichere Datenanalysetechniken und –instrumente zur Verfügung, und die Verknüpfung mit anderen Datensätzen wird einfacher und einfacher, da immer mehr Daten generiert werden. Daher sollten die Organisationen eine periodische Überprüfung ihrer Datenfreigabepolitik und Datenanonymisierungstechniken vornehmen. Außerdem sollten Entscheidungen nie einzig und allein auf aktuelle Bedrohungen gestützt werden – sondern auch auf vorhersehbare künftige Bedrohungen.

Sobald die in Abschnitt 6.4. beschriebene Bewertung der Risiken der Rückidentifizierung vorgenommen und gegebenenfalls auch ein Rückidentifizierungstest durchgeführt wurde, kann die öffentliche Stelle feststellen, ob der Datensatz als anonymisiert eingestuft werden kann oder nicht, mit anderen Worten, ob er keinerlei personenbezogene Daten im Sinne des Artikels 2 Buchstabe a und des Erwägungsgrundes 26 der Richtlinie 95/46/EG mehr enthält. Wenn dem so ist, kann der Datensatz ohne Datenschutzbedingungen freigegeben werden.[28] Andererseits dürfen diese Daten bei erfolgreichem Verlauf eines Tests nicht (oder nicht mehr) als anonymisierte Daten zugänglich gemacht werden, sondern müssen als personenbezogene Daten eingestuft werden (und demzufolge ist ihre Freigabe unter Umständen nicht möglich oder etwa nur nach Maßgabe der in Abschnitt VII erörterten Anforderungen möglich).

6.6. Rückruf der gefährdeten Datensätze

Im Fall einer erwiesenen Rückidentifizierung von Daten aus einem offenen Datensatz muss die öffentliche Stelle, die den Datensatz bereitgestellt hat, in der Lage sein, die Einspeisung abzustellen bzw. den Datensatz von der offenen Datenwebsite zu entfernen. Im Falle der Entfernung des Datensatzes von der Website muss die öffentliche Stelle auch die Rückbenutzer unterrichten und sie auffordern, die Verarbeitung zu stoppen und alle aus dem gefährdeten Datensatz stammenden Daten zu löschen. Da die Unterrichtung aller Rückbenutzer im Rahmen der von der PSI-Richtlinie verlangten offenen Lizenzregelung schwierig sein wird, müssen die öffentlichen Stellen angemessen wirksame Schritte zur Bewältigung dieses Problems unternehmen. Zwar kommt eine Rückrufaktion häufig zu spät, um Schaden zu vermeiden, doch ist sie ein notwendiger Schritt, um mögliche negative Auswirkungen auf die betroffenen Personen abzuschwächen.

[28] Siehe jedoch Abschnitt 10.3 über die 'Lizenzbedingungen für anonymisierte Datensätze', und insbesondere über die Notwendigkeit, Sicherheits- und Schutzmaßnahmen zu ergreifen, um auch weiterhin sicherstellen zu können, dass natürliche Personen nicht rückidentifiziert werden.

VII. Offenlegung personenbezogener Daten zu Zwecken der Weiterverwendung

7.1. Beispiele für öffentlich zugängliche personenbezogene Daten, die von öffentlichen Stellen freigegeben wurden

Zwar ist die Bereitstellung von anonymisierten Datensätzen ein typisches Szenario für Initiativen zur Weiterverwendung von Informationen des öffentlichen Sektors, doch können in einigen Fällen auch öffentliche Stellen personenbezogene Daten zu Zwecken der Weiterverwendung zugänglich machen.

Viele öffentlich zugängliche Register wie Grundbücher oder Handelsregister enthalten große Mengen von personenbezogenen Daten und sind aufgrund von E-Government-Initiativen mehr und mehr auch online zu erreichen. Es gibt auch noch viele andere Beispiele, in denen der Gesetzgeber in einzelnen Mitgliedstaaten eine Rechtsgrundlage für die Bereitstellung personenbezogener Daten von natürlichen Personen im Internet bzw. auf Antrag für den Zugriff auf Dokumente geschaffen hat. Dazu gehören zum Beispiel[29],

- Ausgaben, Besoldung oder Erklärungen zu Interessenskonflikten bei bestimmten öffentlichen Bediensteten oder bei Empfängern von staatlichen Beihilfen (z. B. Agrarsubventionen),
- Namen der Organisationen oder natürlichen Personen, die politischen Parteien Spenden geben,
- Steuererklärungen von natürlichen Personen[30],
- Gerichtsentscheidungen (Namen der Parteien oder anderer natürlicher Personen manchmal gelöscht oder durch Initialen ersetzt, um das Risiko der Rückidentifizierung zu verringern),
- Wählerverzeichnisse,
- Gerichtslisten (z. B. Sitzungspläne der mündlichen Verhandlungen vor Gericht an den Sitzungstagen).

In jedem dieser Fälle können die öffentlichen Stellen oder die Gesetzgeber proaktiv erwägen, ob sie diese Daten zu Zwecken der Weiterverwendung zugänglich machen wollen (z. B. zur Verbesserung der öffentlichen Dienstleistungen, wie z. B. des Zugangs zum Handelsregister oder zum Grundbuch). Potenzielle Weiterverwender können auch Kontakt zu den öffentlichen Stellen aufnehmen und eine Weiterverwendung der Daten beantragen. In einigen anderen Fällen ist es auch möglich, dass potenzielle Weiterverwender einfach nur die personenbezogenen Daten abgreifen, die bereits online zugänglich sind, und sie verwenden, ohne notwendigerweise Kontakt zu der öffentlichen Stelle aufzunehmen, die die betreffenden Informationen freigegeben hat. In allen drei Fällen müssen die Weiterverwender sich selbstverständlich an das Datenschutzrecht halten, da sie mit personenbezogenen Daten umgehen.

7.2. Unterschiede bei den nationalen Zugangsregelungen

Die gesetzlichen Verpflichtungen, bestimmte personenbezogene Daten öffentlich zugänglich zu machen, weichen von Mitgliedstaat zu Mitgliedstaat aufgrund der unterschiedlichen rechtlichen und kulturellen Traditionen stark voneinander ab. In einigen Mitgliedstaaten besteht eine Rechtsgrundlage dafür, bestimmte personenbezogene Daten zugänglich zu machen, während andere Mitgliedstaaten die Offenlegung derselben personenbezogenen Daten in ein und derselben Situation eher verbieten. Die PSI-Richtlinie erkennt dies an und stellt klar, dass sie auf den in den

[29] Siehe auch die in Abschnitt V aufgeführten Beispiele zur Darstellung des Anwendungsbereichs der PSI-Richtlinie.

[30] Siehe beispielsweise das Urteil des Europäischen Gerichtshofs vom 16. Dezember 2008, Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy en Satamedia Oy, C-73/07.

Mitgliedstaaten bestehenden Zugangsregelungen aufbaut und die innerstaatlichen Regelungen für den Zugriff auf Dokumente nicht ändert.[31]

7.3. Notwendigkeit einer Datenschutz-Folgenabschätzung und angemessener Sicherheits- und Schutzmaßnahmen

Wann immer personenbezogene Daten im Regelfall zu Zwecken der Weiterverwendung zugänglich gemacht werden sollen, ist unbedingt auf eine behutsame Vorgehensweise zu achten. Insbesondere empfiehlt die Datenschutzgruppe, dass vor der Veröffentlichung eines Datensatzes (oder vor der Verabschiedung eines Gesetzes, nach dem die Veröffentlichung vorgeschrieben ist) unbedingt eine gründliche Datenschutz-Folgenabschätzung durchgeführt werden muss, in der auch die Möglichkeiten und die potenziellen Auswirkungen der Weiterverwendung zu bewerten sind. Die Offenlegung personenbezogener Daten zu Zwecken der Weiterverwendung im Rahmen einer offenen Lizenz ohne jegliche rechtliche und technische Einschränkungen für die Weiterverwendung ist generell zu vermeiden.

7.4. Wichtigkeit einer Lizenzregelung

Zusätzlich empfiehlt die Datenschutzgruppe, dass eine rigoros Lizenzregelung eingeführt wird, die auch in angemessener Weise durchgesetzt werden muss, um sicherzustellen, dass die personenbezogenen Daten nicht für unvereinbare Zwecke benutzt werden, so z.B. für unerbetene Geschäftsmitteilungen und Werbenachrichten oder auf andere Art und Weise, die die betroffenen Personen als überraschend, unangemessen oder anderweitig verwerflich empfinden.

7.5. Wichtigkeit einer verbindlichen Rechtsgrundlage für die Veröffentlichung und auch für die Weiterverwendung

Die Datenschutzgruppe weist nochmals darauf hin, wie wichtig es ist, eine verbindliche Rechtsgrundlage zu schaffen, nach der personenbezogene Daten öffentlich zugänglich gemacht werden können, und dabei die einschlägigen Datenschutzvorschriften einschließlich der Grundsätze der Verhältnismäßigkeit, der Datensparsamkeit und der Zweckbindung zu berücksichtigen.

Die Datenschutzgruppe empfiehlt, dass jede Rechtsvorschrift, die den öffentlichen Zugang zu bestimmten Daten vorschreibt, eine eindeutige Zweckbestimmung für die Offenlegung personenbezogener Daten vornimmt. Erfolgt dies nicht oder nur in allgemeinen und vagen Formulierungen, dann nimmt die Rechtssicherheit und die Berechenbarkeit Schaden. Insbesondere in Bezug auf einen Antrag auf Gestattung der Weiterverwendung wird es für die öffentliche Stelle und die betreffenden potenziellen Weiterverwender sehr schwierig zu ermitteln, welche Zwecke ursprünglich mit der Veröffentlichung verfolgt wurden, und welche weiteren Zielsetzungen in der Folge mit diesen ursprünglich verfolgten Zwecken vereinbar wären. Wie bereits erwähnt, ist, auch wenn die personenbezogenen Daten im Internet veröffentlicht wurden, nicht davon auszugehen, dass sie zu allen möglichen Zwecken weiterverarbeitet werden dürfen.

Jede weitere Weiterverwendung muss in diesen Fällen auf einen geeigneten Rechtsgrund im Rahmen von Artikel 7 Buchstabe a bis f der Richtlinie 95/46/EG gestützt werden können (z. B. Zustimmung oder kraft Gesetzes) und mit allen anderen Datenschutzgrundsätzen im Einklang stehen.

[31] Demnach muss das innerstaatliche Recht, wie bereits in Abschnitt 5.4. erläutert, nach wie vor mit Artikel 8 EMRK und den Artikeln 7 und 8 der EU-Charta in der jeweiligen Auslegung durch die ständige Rechtsprechung im Einklang stehen.

7.6. Zweckbindung

Die wirkungsvolle Umsetzung des Grundsatzes der Zweckbindung stellt im Falle der Weiterverwendung von Informationen des öffentlichen Sektors (PSI) eine Herausforderung dar. Einerseits ist die eigentliche Idee und die treibende Kraft für Innovation, die hinter dem Konzept der 'offenen Daten' und der Weiterverwendung von Informationen des öffentlichen Sektors steht, die, dass die Informationen zu Zwecken der Weiterverwendung für innovative neue Produkte und Dienstleistungen und somit für Zwecke bereitstehen sollten, die nicht vorab festgelegt wurden und die nicht eindeutig vorhergesehen werden können. Die PSI-Richtlinie verlangt auch, dass bei einer Lizenzvergabe die Weiterverwendung nicht unnötig eingeschränkt werden soll.

Andererseits handelt es sich bei der Zweckbindung um ein Grundprinzip des Datenschutzes, das verlangt, dass die für einen bestimmten Zweck erhobenen personenbezogenen Daten nicht für einen anderen, unvereinbaren Zweck weiterverwendet werden dürfen.[32] Dieser Grundsatz gilt auch für personenbezogene Daten, die öffentlich zugänglich sind. Die bloße Tatsache, dass personenbezogene Daten für einen bestimmten Zweck öffentlich zugänglich sind, bedeutet nicht, dass diese personenbezogenen Daten zu Zwecken der Weiterverwendung für einen anderen Zweck offen sind.

Beispielsweise werden die Spesen von ranghohen Regierungsbeamten der Transparenz halber im Internet zugänglich gemacht, aber deren Weiterverwendung durch einen Bürger für andere Zwecke ist nicht vereinbar.

Wie in der Stellungnahme 3/2013 der Datenschutzgruppe zur Zweckbindung eingehender erörtert wurde (siehe Abschnitt III.2.2 und Anhang 1) verlangt die Beurteilung, ob die Weiterverarbeitung von personenbezogenen Daten mit den Zwecken unvereinbar ist, für die diese Daten erhoben wurden, eine Bewertung unter Berücksichtigung vieler Faktoren. Berücksichtigung finden insbesondere

(a) das Verhältnis zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken einer Weiterverarbeitung;
(b) der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, mit den berechtigten Erwartungen der betroffenen Personen hinsichtlich ihrer weiteren Verwendung;
(c) die Art der personenbezogenen Daten und die Auswirkungen der Weiterverarbeitung auf die betroffenen Personen;
(d) die vom für die Verarbeitung Verantwortlichen ergriffenen Sicherheits- und Schutzmaßnahmen zur Gewährleistung einer fairen Verarbeitung und zur Verhütung von unangemessenen Auswirkungen auf die betroffenen Personen.

Diese Schlüsselfaktoren sind bei der Entscheidung zu bewerten, ob personenbezogene Daten offengelegt werden sollen, wie auch in jedem Fall, in dem personenbezogene Daten weiterverwendet werden. Nachstehend sind einige Beispiele dafür aufgeführt:

- Eine öffentliche Stelle veröffentlicht Kontaktdaten, u. a. Name, Titel, Anschrift der Dienststelle und dienstliche Telefonnummer ihrer Beamten in einem Dienststellenverzeichnis. Der offensichtliche – obwohl nicht extra genannte – Zweck dieses Verzeichnisses besteht darin, dem Bürger bei der Auswahl seines Ansprechpartners für

[32] Nur in Ausnahmefällen – nach Maßgabe der strengen Sicherheits- und Schutzmaßnahmen gemäß Artikel 13 der Richtlinie 95/46/EC – können Daten auf eine Weise verwendet werden, die mit den bei ihrer Erhebung angegebenen Zwecken unvereinbar ist. Siehe dazu Abschnitt III.3 der Stellungnahme 3/2013 der Datenschutzgruppe zur Zweckbindung.

amtliche Anfragen und andere Amtsgeschäfte zu helfen. Ein Weiterverwender möchte gerne den Inhalt dieses Verzeichnisses 'ernten', ihn mit den Privatanschriften und –telefonnummern der öffentlichen Bediensteten kombinieren (sofern diese öffentlich zugänglich sind, z. B. in einem Telefonbuch) und sowohl Privat- als auch Dienstanschriften und –telefonnummern auf einer interaktiven Karte veröffentlichen, um zu zeigen, wo die verschiedenen Beamten wohnen und arbeiten. Diese Datenkombination und Weiterverwendung ist als mit dem ursprünglichen Zweck unvereinbar anzusehen. Ein Beamter, dessen dienstliche Kontaktdaten veröffentlicht werden, damit ihn die Bürger ansprechen können, hätte nicht halbwegs damit gerechnet, dass diese Informationen dann mit anderen Daten verknüpft werden, die er aber zu einem anderen Zweck, der nicht mit seiner Arbeit zusammenhängt, öffentlich zugänglich gemacht hat.

- In einigen Mitgliedstaaten sind die Ankündigungen einer geplanten Heirat nach innerstaatlichem Recht öffentlicher Natur und können von jedermann eingesehen werden. Ein solches Aufgebot stellt auf die Bekanntgabe des Heiratswillens des verlobten Paares und auf die Möglichkeit für Interessenten ab, dieser Heirat zu widersprechen. Die Tatsache, dass die in der Veröffentlichung der Heiratsankündigung enthaltenen personenbezogenen Daten jedermann zugänglich sind, gibt Dritten jedoch nicht das Recht, diese Informationen für die Zusendung von kommerziellen Mitteilungen an das Paar zu nutzen. Diese zusätzliche Nutzung ist unvereinbar, da der Zweck von Aufgeboten nach den gesetzlichen Vorschriften darin zu sehen ist, das Vorbringen von Einwänden gegen die Heirat zu ermöglichen.

7.7. Kommerzielle gegen nichtkommerzielle Zwecke

Die Stellungnahme 7/2003 hebt die kommerziellen Tätigkeiten als wichtigsten Beweggrund für die Weiterverwendung von Informationen des öffentlichen Sektors hervor, während beim Zugang zu Informationen die Gesetze über die Informationsfreiheit den Zweck in der Sicherstellung von Transparenz, Offenheit und Verantwortlichkeit gegenüber den Bürgern sehen.

Die Stellungnahme 7/2003 betont auch, dass die Bürger ‘im Normalfall die Informationen für ihre eigenen, nichtkommerziellen Zwecke’ nutzen. Diese Feststellung muss angesichts der inzwischen mit der Weiterverwendung von Informationen des öffentlichen Sektors gemachten Erfahrungen aktualisiert werden. Die Erfahrungen mit Open-Data-Initiativen haben gezeigt, dass die Weiterverwendung von Informationen des öffentlichen Sektors mitunter auch erheblich zur Stärkung der Transparenz und Verantwortlichkeit beiträgt und zu einer besseren Nutzung der öffentlichen Dienstleistungen führt. Die Unterscheidung zwischen der Weiterverwendung für kommerzielle und der für nichtkommerzielle Zwecke sollte für die Betrachtung der weiteren Nutzung von personenbezogenen Daten nicht entscheidend sein. Die Bewertung der Vereinbarkeit sollte nicht in erster Linie darauf beruhen, ob sich das Wirtschaftsmodell eines potenziellen Weiterverwenders auf Gewinne stützt oder nicht.

Was sorgfältig bewertet werden muss ist die Frage, ob die Zwecke und die Wege, nach denen Daten weiterverarbeitet werden, mit den ursprünglichen Zwecken nach den in Abschnitt 7.6. aufgeführten Kriterien vereinbar sind. Im Fall der Weiterverwendung von Informationen des öffentlichen Sektors wird dies unweigerlich zur Berücksichtigung nicht nur eines, sondern eher einer Reihe von Verarbeitungsszenarios führen.

7.8. Verhältnismäßigkeit und andere Belange

Ein weiterer wichtiger Grundsatz gemäß der Richtlinie 95/46/EG ist die Verhältnismäßigkeit[33]. Es gibt mehrere verschieden Methoden und Vorgehensweisen, wie man personenbezogene Daten öffentlich zugänglich macht. Einige davon sind mitunter etwas einschneidender als andere und bieten größere Risiken. Folglich sind manche als verhältnismäßig anzusehen während andere dies nicht sind.

Wie schon beim Zweck gibt es auch hier Besorgnis, wie die Weiterverarbeitung von Daten zu kontrollieren und die Einhaltung der anderen Grundsätze des Datenschutzrechts, so auch der Verhältnismäßigkeit, aber nicht auf diese beschränkt, sicherzustellen ist. Sobald die Daten öffentlich zugänglich sind, besonders im Internet, ist es sehr schwierig, ihre Verwendung wirksam zu begrenzen und die Einhaltung der Datenschutzgesetze zu gewährleisten.

Zu den Herausforderungen, wie die Einhaltung der Datenschutzgesetze zu gewährleisten ist, gehören die Überlegungen

- wie Aktualisierung und Fehlerfreiheit der von der Primärquelle abgekoppelten Daten sicherzustellen sind;
- wie sicherzustellen ist, dass die Nutzung personenbezogener Daten auf die Funktionalitäten beschränkt bleibt, die als ursprünglicher Zweck ihrer Veröffentlichung vorgesehen waren;
- wie die zeitgerechte Löschung der Daten sicherzustellen ist, wenn die Veröffentlichung der der personenbezogenen Daten nur für einen begrenzten Zeitraum vorgesehen war[34];
- wie die Rechte der natürlichen Personen in Bezug auf die zu Zwecken der Weiterverwendung bereitgestellten personenbezogenen Daten auszuüben sind (einschließlich der Rechte auf Berichtigung, Aktualisierung und Löschung).

7.9. Rechtliche und/oder technische Einschränkungen der Weiterverwendung

Manchmal beschränkt eine Rechtsvorschrift oder die technische Gestaltung des Systems spezielle Verarbeitungsvorgänge oder errichtet andere Sicherheits- und Schutzmaßnahmen, die die Nutzung von öffentlichen Registern einschränken (z. B. Begrenzung der Möglichkeit, den gesamten Inhalt des Registers herunterzuladen oder Einschränkung der Suchfunktionen, beispielsweise auf der Grundlage des Vor- und Nachnamens einer natürlichen Person). In diesem Fall ist die Weiterverwendung grundsätzlich nur nach Maßgabe dieser speziellen Bedingungen und Einschränkungen gestattet.

In diesem Zusammenhang kommt es darauf an, sorgfältig zu überlegen, welche Maßnahmen – einschließlich rechtlicher und technischer Maßnahmen – durchgeführt werden könnten, um sicherzustellen, dass auf die Datenschutzbelange, einschließlich der in Abschnitt 7.8. dargestellten Belange, eingegangen wird. Es kommt besonders darauf an, wie die Weiterverwender auf die Daten zugreifen können – z. B. mittels einer Massen-Download-Funktion oder im Wege einer benutzerdefinierten Schnittstelle mit begrenzten Zugriffsmöglichkeiten nach Maßgabe bestimmter Bedingungen. Diesbezüglich ist von entscheidender Bedeutung, welche zusätzlichen

[33] Siehe Artikel 6 Absatz 1 Buchstabe c der Richtlinie 95/46/EG.

[34] Siehe beispielsweise Urteil des Gerichtshofs vom 9. November 2010, Volker und Markus Schecke GbR /. Land Hessen, Verbundene Rechtssachen C-92/09 und C-93/09, Randnr. 31: 'Im Übrigen sei es nicht möglich, die Daten nach Ablauf des in Art. 3 Abs. 3 der Verordnung Nr. 259/2008 vorgesehenen Zeitraum von zwei Jahren aus dem Internet zu entfernen'.

Sicherheitskontrollen vorgenommen werden, wie z. B. der Einsatz eines 'Captcha[35]'-Verifikationssystems zur Verhinderung des automatisierten Zugriffs und zur Minimierung des Risikos, dass eine gesamte Datenbank abgeerntet wird. Mittels spezifischer technischer Maßnahmen können Missbrauch von personenbezogenen Daten und negative Auswirkungen auf betroffene Personen minimiert werden, die ansonsten durch unbeschränkte und vorbehaltslose Zugriffe von Weiterverwendern auf komplette Datensätze ermöglicht würden.

In vielen Fällen kann es vor allem nötig sein, sicherzustellen, dass die Weiterverwender nur zielgerichtete Anfragen stellen können, und zwar mithilfe von Technologien, die dazu dienen, Massen-Downloads von Datensätzen zu verhindern, so z. B. durch auf die Kundenbedürfnisse zugeschnittene Anwendungs-Programmierschnittstellen ('APIs'). Damit kann die Verhältnismäßigkeit der Nutzung und die Minimierung des Risikos des Missbrauchs kompletter Datenbanken sichergestellt werden. Zudem helfen diese speziell zugeschnittenen Schnittstellen sicherzustellen, dass die Daten immer aktualisiert werden, und auch, dass die Daten nicht mehr über die API abrufbar sind, sobald die betreffende öffentliche Stelle die entsprechende Entscheidung trifft. Andererseits kann sie die Möglichkeiten beschränken, wie ein Weiterverwender die Daten weiterverwenden kann.

7.10. Fehlerfreiheit, Aktualisierung und Löschung

Eine weitere spezielle Frage ist, was passiert, wenn personenbezogene Daten nur für einen befristeten Zeitraum veröffentlicht oder anderweitig öffentlich zugänglich gemacht werden. Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG bestimmt, dass personenbezogene Daten 'nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden müssen, die die Identifizierung der betroffenen Person ermöglicht'. Erwägungsgrund 18 der PSI-Richtlinie bestimmt: 'Entscheidet sich die zuständige Behörde, bestimmte Dokumente nicht mehr für die Weiterverwendung zur Verfügung zu stellen oder diese Dokumente nicht mehr zu aktualisieren, so sollte sie diese Entscheidung so bald wie möglich, möglichst auf elektronischem Weg, bekannt geben'.

Es ist jedoch schwierig oder manchmal unmöglich, sicherzustellen, dass die Daten gelöscht oder beseitigt werden, sobald sie erst einmal veröffentlicht und für die Weiterverwendung zur Verfügung gestellt worden sind.

In dieser Hinsicht kann es vielleicht schon zu einer Lösung beitragen – wenn auch nicht voll und ganz – wenn die Daten nicht in einer herunterladbaren Form bereitgestellt werden, sondern nur über eine speziell zugeschnittene API und nach Maßgabe bestimmter Einschränkungen und Sicherheitsmaßnahmen, wie oben dargelegt.

VIII. Forschungsdaten

Hier ist es wichtig, zwischen der Veröffentlichung anonymisierter Daten einerseits (siehe Abschnitt VI) und dem beschränkten Zugang andererseits zu unterscheiden. Zweifelsohne ist die Open-Data-Agenda auf die öffentliche Verfügbarkeit der Daten angewiesen. Jedoch findet viel

[35] CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) ist ein Challenge-Response-Systemtest (etwa: Aufforderung-Antwort-Systemtest), der so konzipiert ist, dass er menschliches Verhalten von automatisierten Programmen unterscheiden kann. Ein CAPTCHA differenziert also zwischen einem Menschen und einem Computer, indem er eine Aufgabe stellt, die von den meisten Menschen leicht, aber für die derzeitigen Computerprogramme eher schwer zu lösen ist.

Forschungsarbeit (vor allem naturwissenschaftliche Forschung, sowohl für kommerzielle als auch nichtkommerzielle Zwecke, aber auch andere Forschung) statt, indem Daten innerhalb einer geschlossenen Gemeinschaft freigegeben werden, h. h., dort, wo nur eine begrenzte Anzahl von Forschern bzw. Forschungseinrichtungen Zugang zu den Daten hat, und wo es möglich ist, die weitere Offenlegung oder Verwendung der Daten einzuschränken, und wo ihre Sicherheit garantiert werden kann.

Die Beschränkung des Zugangs ist besonders wichtig bei der Behandlung von personenbezogenen Daten (häufig in pseudonymisierter Form[36]), die aus sensiblem Quellenmaterial abgeleitet wurden oder bei denen ein erhebliches Rückidentifizierungsrisiko besteht. Auch bei einer im Rahmen der Beschränkung des Zugangs erfolgenden Offenlegung können immer noch Risiken vorhanden sein – diese sind aber niedriger und können besser entschärft werden, wenn die Daten in einer geschlossenen und nach gefestigten Regeln arbeitenden Gemeinschaft offengelegt werden.

Ein Problem, mit dem diejenigen häufig konfrontiert sind, die Daten für Forschungszwecke nutzen, besteht darin, dass sie einerseits Daten haben wollen, die ergiebig, detailgenau untergliedert und für ihre Zwecke direkt verwertbar sind; andererseits wollen sie aber auch sicherstellen, dass keine Rückidentifizierung von natürlichen Personen erfolgt. Am einen Ende des Spektrums können auf individueller Ebene pseudonymisierte (z. B. einfach verschlüsselte) Daten für die Forscher sehr wertvoll sein, und zwar wegen ihrer individuell gestalteten Granularität, und weil sich pseudonymisierte Datensätze, die von verschiedenen Quellen stammen, relativ leicht abgleichen und zusammenführen lassen. Dies bedeutet jedoch auch, dass ein hohes Rückidentifizierungsrisiko besteht: die Möglichkeit, mehrere Datensätze (pseudonymisiert oder nicht) mit ein und derselben natürlichen Person in Zusammenhang zu bringen, kann ein Wegbereiter für die Identifizierung sein oder sogar unmittelbar die Identifizierung möglich machen.

Daher ist vor einer Veröffentlichung oder Bereitstellung von pseudonymisierten Datensätzen zu Zwecken der Weiterverwendung ein höheres Maß an genauer Prüfung und an zusätzlicher Vorsicht geboten. Generell gilt, dass je detaillierter, verknüpfbarer und individueller gestaltet die Daten sind, desto eingeschränkter und kontrollierter sollte der Zugang zu den Daten sein. Je aggregierter und weniger verknüpfbar die Daten sind, desto wahrscheinlicher wird, dass sie ohne erhebliche Risiken veröffentlicht und zu Zwecken der Weiterverwendung bereitgestellt werden können.

Dabei handelt es sich um ein kompliziertes und sich weiterentwickelndes Gebiet, und es wäre unangemessen, die Veröffentlichung und die Weiterverwendung aller Datensätze, die der in Abschnitt VI beschriebenen hohen Schwelle der 'Anonymisierung' nicht gerecht werden, kategorisch auszuschließen. Angesichts dessen, und obwohl ja als Faustregel eine Einzelfallanalyse und eine sorgfältige Bewertung immer erforderlich ist, ist die Datenschutzgruppe der Auffassung, dass im Allgemeinen eine Freigabe von individuell gestalteten Datensätzen oder von anderen Datensätzen, die ein erhebliches Rückidentifizierungsrisiko darstellen, im Rahmen der Bestimmungen der PSI-Richtlinie oft nicht angemessen sein wird.

Außerdem ist es wichtig, den folgenden Zusammenhang hervorzuheben: Sollte ein solcher Datensatz nach einer sorgfältigen Bewertung der Vorteile und der Risiken trotzdem veröffentlicht und für die Weiterverwendung bereitgestellt werden, so muss die Offenlegung und jede weitere Weiterverwendung in vollkommener Übereinstimmung mit dem Datenschutzrecht erfolgen (siehe

[36] Siehe Stellungnahme 4/2007 zum Begriff "personenbezogene Daten", angenommen am 20. Juni 2007 (WP 136), insbesondere S. 14-24 (wobei 'pseudonymisierte Daten', 'verschlüsselte Daten' und 'anonyme Daten' auf S. 21-24 abgehandelt werden). Das Thema Informationen 'über' eine natürliche Person wird auf S. 10-14 behandelt. Relevant ist auch, wie auf Seite 3 angemerkt, dass die Datenschutzgruppe derzeit an der Bereitstellung weiterer Leitlinien zu Anonymisierungstechniken arbeitet.

Abschnitt VII). Dies ist so, weil diese Daten, auch wenn einige (manchmal sogar sehr erhebliche) Maßnahmen zur Verringerung der Risiken einer Rückidentifizierung unternommen wurden, trotzdem auch weiterhin als personenbezogene Daten gelten.

IX. Historische Archive

Historische Archive und Museen weisen ebenfalls spezifische Charakteristika auf, die spezielle Sicherheits- und Schutzmaßnahmen erforderlich machen. In vielen Fällen und je nach Faktoren, wie Alter und Sensibilität der Daten sowie dem Zusammenhang der Datenerhebung, können andere Optionen – wie z, B. die Bewilligung des eingeschränkten Zugangs nach Maßgabe von Verschwiegenheitspflichten – angemessener sein als die Digitalisierung und die uneingeschränkte Bereitstellung der Daten im Internet zu Zwecken ihrer Weiterverwendung.

In Bezug auf Archives gilt es noch auf Folgendes hinzuweisen: Zwar nimmt die Datensensibilität im Laufe der Zeit im Allgemeinen ab, doch kann auch eine unangemessene Freigabe von viele Jahrzehnte alten Datensätzen nach wie vor ernsthafte nachteilige Auswirkungen auf die natürliche Person haben, die unmittelbar davon betroffen ist, aber auch auf andere natürliche Personen, wie z. B. die Familienangehörigen oder die Nachfahren. Dies trifft insbesondere auf hochsensible Daten zu. Beispielsweise würden freigegebene Strafregisterauszüge eine natürliche Person weiterhin stigmatisieren und sie bei ihrer Rehabilitation behindern. Ferner können Informationen, dass eine bereits verstorbene natürliche Person ein Geheimdienstmitarbeiter oder ein Kollaborateur eines Unterdrückerregimes, ein Pädophiler oder ein Verbrecher war, an einer stigmatisierenden Geisteskrankheit oder an einer Erbkrankheit litt, ebenso allesamt negative Auswirkungen auf die Familie der verstorbenen Person haben (z. B. den überlebenden Ehegatten, die Kinder oder andere Nachfahren). DNA-Proben von verstorbenen natürlichen Personen, die manchmal in den Archiven von öffentlichen Krankenhäusern aufbewahrt werden, können aus ähnlichen Gründen Schutzmaßnahmen erforderlich machen. Daher verlangen solche Informationen, auch wenn sie sich auf Verstorbene beziehen, unter Umständen, dass Schutzmaßnahmen nach den Datenschutzgesetzen und/oder gegebenenfalls nach anderen Gesetzen zum Schutz der Grundrechte ergriffen werden.

Oft haben die Mitgliedstaaten spezielle Gesetze zur Regelung des Zugangs zu nationalen Archiven, zu historischen Archiven über die jüngste Vergangenheit von besonderem Interesse (wie z. B. Archiven, in denen Beweismaterial über die Kollaboration mit Unterdrückerregimen aufbewahrt wird), und zu Archiven, die der Aufbewahrung der Justizakten dienen.[37] Diese Gesetze schreiben häufig angemessene Sicherheitsmaßnahmen und Zugangsbeschränkungen sowie weitere Schutzmaßnahmen vor, die auf die Güterabwägung und den Ausgleich der auf dem Spiel stehenden Interessen und auf die Gewährleistung der Zugangsmöglichkeit zu bestimmten personenbezogenen Daten zu Zwecken der Geschichtsforschung, der Transparenz und der journalistischen Recherche abstellen und gleichzeitig darauf achten, dass Offenlegungen, wenn sie denn erforderlich sind, in engen Grenzen erfolgen, damit sie nicht das Privat- und Familienleben und die Würde der betreffenden Parteien beeinträchtigen können.

In Bezug auf den Grundsatz der ‘Zweckbindung’ ist festzustellen, dass historische Archive üblicherweise Informationen zu Zwecken der Geschichtsforschung beherbergen. Diese Zwecke unterscheiden sich von den ursprünglichen Zwecken, für die Daten erhoben wurden. Die

[37] Als noch andere Beispiele wären u. a. die Archive der Personenstandsregister zu nennen, die in manchen Mitgliedstaaten u. a. folgende Angaben enthalten: Todesursache, Geschlechtsumwandlung, Name des Partners (von dem sich auf die sexuelle Ausrichtung schließen lässt) oder die Tatsache, dass eine natürliche Person adoptiert wurde. Der Zugang zu diesen Archiven unterliegt ebenfalls besonderen Bedingungen.

Materialien, die schließlich in Archivsammlungen enden, wurden ursprünglich von den verschiedenen öffentlichen Stellen zu bestimmten Verwaltungszwecken erstellt. Üblicherweise wird nach einem bestimmten Zeitraum, wenn das betreffende Dokument für die ursprünglichen Verwaltungszwecke nicht mehr gebraucht wird, ein Aussonderungsverfahren durchgeführt, und die Dokumente, die als von 'historischem' Wert gelten, werden in die historischen Archive überführt. Hier stellt sich die Frage, zu welchen Zwecken die in den historischen Archiven eingelagerten personenbezogenen Daten für eine Weiterverwendung bereitgestellt werden sollen. In diesem Zusammenhang muss eine sorgfältige Bewertung vorgenommen werden, bei der der potenzielle Wert der Bereitstellung von Archivmaterial zu Zwecken der Weiterverwendung einerseits, andererseits aber auch die potenziellen Auswirkungen auf die Rechte, die Freiheiten und die Würde der betroffenen Personen zu berücksichtigen sind.

Alles in allem lässt sich schlussfolgern, dass zwar die Digitalisierung bestimmter Datensätze, die personenbezogene Daten enthalten, und deren Bereitstellung zu Zwecken der Weiterverwendung in manchen Situationen angebracht sein mag, und dass einige Daten auch in anonymisierter Form freigegeben werden können, dass in anderen Fällen aber Beschränkungen für die Offenlegung und die Weiterverwendung von personenbezogenen Daten und angemessene Sicherheitsmaßnahmen zum Schutz dieser Daten von größter Bedeutung sind. Eine gründliche Datenschutz-Folgenabschätzung muss sicherstellen, dass keine Archivsammlung zu Zwecken der Weiterverwendung bereitgestellt wird, sofern nicht potenzielle Negativauswirkungen auf die betroffenen natürlichen Personen ausgeschlossen bzw. derartige Risiken auf ein annehmbares Mindestmaß reduziert werden können. Der Archivsektor könnte auch erwägen, entsprechende Verhaltenskodexe auszuarbeiten bzw. vorhandene Kodexe um die Darstellung bewährter Verfahrensweisen zu ergänzen.

X. Lizenzvergabe für personenbezogene Daten zu Zwecken der Weiterverwendung

10.1. Relevante Bestimmungen der PSI-Richtlinie

Erwägungsgrund 15 der PSI-Richtlinie enthält folgende Zielvorgaben: 'Die Gewährleistung der Klarheit und öffentlichen Verfügbarkeit der Bedingungen für die Weiterverwendung von Dokumenten des öffentlichen Sektors ist eine Voraussetzung für die Entwicklung eines gemeinschaftsweiten Informationsmarktes. Daher sollten alle geltenden Bedingungen für die Weiterverwendung von Dokumenten allen potenziellen Weiterverwendern erläutert werden. Die Mitgliedstaaten sollten zur Unterstützung und Erleichterung der Anträge auf Weiterverwendung die Anlage von gegebenenfalls online zugänglichen Verzeichnissen der verfügbaren Dokumente fördern'.

Ferner enthält Erwägungsgrund 26 der PSI-Änderungsrichtlinie folgende Regelung: 'In Verbindung mit einer Weiterverwendung des Dokuments kann die öffentliche Stelle dem Weiterverwender – gegebenenfalls durch eine Lizenz – Bedingungen auferlegen ...' […] 'Deshalb sollten die Mitgliedstaaten die Verwendung offener Lizenzen' in maschinenlesbaren Formaten fördern.

Ferner bestimmt Artikel 8 Absatz 1: 'Öffentliche Stellen können die Weiterverwendung ohne Bedingungen gestatten oder aber, gegebenenfalls im Rahmen einer Lizenz, Bedingungen festlegen. Diese Bedingungen dürfen die Möglichkeiten der Weiterverwendung nicht unnötig einschränken und nicht der Behinderung des Wettbewerbs dienen.'

10.2. Lizenzvergabe und Datenschutz

Lizenzen sind das Kernstück der PSI-Regelung. Sie können sich auch auf die Art und Weise auswirken, wie personenbezogene Daten verarbeitet werden, und sollten zu den Sicherheits- und

Schutzmaßnahmen zählen, die anzuwenden sind, wenn personenbezogene Daten (oder aus personenbezogenen Daten abgeleitete anonymisierte Daten) zu Zwecken der Weiterverwendung bereitgestellt werden. Durch Lizenzen erübrigt sich nicht das Erfordernis der Vereinbarkeit mit dem Datenschutzrecht, aber eine Datenschutzklausel in den Lizenzbedingungen wäre hilfreich, um die Vereinbarkeit mit dem Datenschutzrecht zu gewährleisten, da mit ihr eine zusätzliche Ebene der 'Durchsetzbarkeit' hinzugefügt wird. Eine solche Klausel könnte auch das Bewusstsein schärfen helfen, indem sie die Weiterverwender an ihre Pflichten als für die Verarbeitung der Daten Verantwortliche erinnert.

Hinsichtlich des Inhalts dieser Lizenzen macht es Sinn, zwischen zwei verschiedenen Szenarios zu unterscheiden.

10.3. Lizenzbedingungen für anonymisierte Datensätze

In Bezug auf die anonymisierten Daten (d. h. Datensätze, die keinerlei personenbezogene Daten mehr enthalten) sollten die Lizenzbedingungen zunächst

- wiederholen, dass die Datensätze anonymisiert wurden;
- den Lizenzinhabern die Rückidentifizierung von natürlichen Personen verbieten[38];
- den Lizenzinhabern untersagen, die Daten für eine Maßnahme oder eine Entscheidung in Bezug auf die betreffenden natürlichen Personen zu verwenden, und
- auch die Verpflichtung enthalten, nach der die Lizenzinhaber dem Lizenzgeber mitteilen müssen, wenn entdeckt wird, dass die natürlichen Personen rückidentifiziert werden können oder bereits rückidentifiziert worden sind.

Als Alternative zu der Lizenzbedingung könnte den Weiterverwendern eine Warnmeldung in klar erkennbarer Form auf dem Open-Data-Portal zur Kenntnis gebracht werden. Jedoch sollte die Annahme der Lizenzbedingungen gefördert werden, weil diese den zusätzlichen Vorteil der vertraglichen Durchsetzbarkeit haben.

Rückruf der gefährdeten Datensätze

Die Möglichkeit, den Lizenzgeber auf die Tatsache aufmerksam zu machen, dass eine Rückidentifizierung stattgefunden hat oder stattfinden kann, muss allen anderen Web-Benutzern zur Verfügung stehen, so auch den betroffenen Personen selbst. Wird ein erhöhtes Rückidentifizierungsrisiko vom Lizenzgeber entdeckt, sollte in der Lizenz ein Verfahren vorgesehen sein, mit dem der Lizenzgeber eine 'Rückrufaktion' für den 'gefährdeten' Datensatz in Gang setzen kann. Mit anderen Worten, die Datenschutzklausel sollte dem Lizenzgeber das Recht an die Hand geben, die Zugangsmöglichkeit zu den Daten auszusetzen oder zu beenden (z. B. das Recht, die APT-Schnittstelle abzuschalten oder die Datei aus der Plattform zu entfernen). Der Lizenzgeber muss alle zumutbaren Anstrengungen unternehmen, um sämtliche Weiterverwender dazu aufzufordern, alle Datensätze, die gefährdet sind (rückidentifizierbar wurden), ganz oder teilweise zu löschen. Dazu gehören Mitteilungen in klar erkennbarer Form auf Websites, wie z. B. Open-Data-Portalen und Foren/E-Mail-Listen/Social Media, die von solchen natürlichen Personen oder Gruppen

[38] In begrenztem Umfang können Ausnahmen zum Tragen kommen, so z. B. in Fällen eines gutgläubigen Testens der Rückidentifizierung. Selbst in solchen Fällen sollten die Testergebnisse jedoch dem für die Verarbeitung Verantwortlichen und der betreffenden öffentlichen Stelle zur Kenntnis gebracht werden, und die rückidentifizierten Daten nicht veröffentlicht oder anderweitig weiterverbreitet werden.

aufgerufen werden, die wahrscheinlich diese Daten weiterverwenden. Das effektivste Mittel für den Rückruf von Datensätzen besteht wahrscheinlich in der Pflicht, sich registrieren zu lassen, aber diese Möglichkeit sollte nicht gefördert werden, wenn dafür wieder neue personenbezogene Daten von den Weiterverwendern erhoben werden müssen und dies im Allgemeinen eine abschreckende Wirkung für die Nutzung von PSI-Websites und anderen Diensten hätte.

10.4. Lizenzbedingungen für personenbezogene Daten

Wenn eine Lizenz für personenbezogene Daten vergeben wird, müssen Grenzen für die Verwendung solcher Daten definiert werden. Dabei kommt es vorrangig darauf an, sicherzustellen, dass jegliche Weiterverwendung auf das Maß beschränkt wird, das 'mit den Zwecken vereinbar ist, für die die Daten ursprünglich erhoben wurden'.[39] Um dies zu erreichen, müssen die Lizenzbedingungen zumindest klarstellen, zu welchen Zwecken die Daten zuerst veröffentlicht wurden, und Anhaltspunkte dafür liefern, was als mit der Verwendung personenbezogener Daten vereinbar angesehen wird und was nicht.

Es ist jedoch festzuhalten, dass dies 'nicht unnötig die Möglichkeiten für die Weiterverwendung einschränken' sollte (Artikel 8 Absatz 1 der PSI-Änderungsrichtlinie). Dies kann häufig bedeuten, dass die Gattungsbegriffe der offenen Standardlizenzen nicht passend sind und für bestimmte personenbezogene Daten spezielle Lizenzen entwickelt werden müssen bzw. Mustervorlagen benutzt werden dürfen, die angepasst werden können.

Zur Zeit sind bei einigen offenen Standardlizenzen (wie z. B. der UK open government licence) personenbezogene Daten ausgeschlossen – nach deren Bedingungen wird für sie überhaupt keine Lizenz vergeben.

10.5. Robuste Durchsetzung sollte die Folge sein, wenn eine Rückidentifizierung oder eine unvereinbare Verwendung vorkommt

Wenn die Daten im Rahmen einer Lizenz veröffentlicht wurden – wie z. B. einer Lizenz für offene Verwaltungsdaten (open government licence) – kann es schwierig sein, sie vor weiterer unvereinbarer Verwendung oder Offenlegung zu schützen oder sie in Sicherheit zu halten. Die Überwachung der Weiterverwendung und die Durchsetzung des Rechts gegen Verletzungen, sei es in Form der Rückidentifizierung von betroffenen Personen oder der weiteren Verwendung für unvereinbare Zwecke, durch den Lizenzgeber ist in diesem Zusammenhang sehr wichtig.

Zwar weist die Datenschutzgruppe wiederholt auf die wichtige Rolle hin, die die öffentlichen Stellen spielen sollten, doch betont sie auch, dass wenn ein Weiterverwender personenbezogene Daten im Rahmen eines Rückidentifizierungsverfahrens erhebt, dieser Weiterverwender höchstwahrscheinlich so angesehen wird, dass er rechtswidrig personenbezogene Daten verarbeitet und damit Durchsetzungsmaßnahmen der Datenschutzbehörden unterliegt. Dazu gehören nach dem Vorschlag für eine Datenschutzverordnung hohe Geldstrafen.

XI. Schlussfolgerungen

Abschließend wiederholt die Artikel-29-Datenschutzgruppe, dass die Weiterverwendung von Informationen des öffentlichen Sektors (PSI) Vorteile bringen kann, die zu größerer Transparenz und zur innovativen Weiterverwendung von Informationen des öffentlichen Sektors führt. Die sich daraus ergebenden größeren Zugangsmöglichkeiten zu Informationen sind jedoch nicht ohne

[39] Siehe Stellungnahme 3/2013 der Datenschutzgruppe zur Zweckbindung.

Risiken. Um den Schutz der Privatsphäre und der personenbezogenen Daten der natürlichen Personen sicherstellen zu können, muss ein ausgewogenes Konzept verfolgt werden, und das Datenschutzrecht muss dabei helfen, den Auswahlprozess, welche personenbezogenen Daten zu Zwecken der Weiterverwendung bereitgestellt werden können und welche nicht, und welche Maßnahmen zum Schutz von personenbezogenen Daten ergriffen werden sollen, in die richtigen Bahnen zu lenken.

Unbeschadet des in der PSI-Änderungsrichtlinie formulierten 'Grundsatzes der Weiterverwendbarkeit' ist die Weiterverwendung zu kommerziellen und nichtkommerziellen Zwecken im Rahmen der Bestimmungen der PSI-Richtlinie nicht immer angemessen, wenn die Informationen des öffentlichen Sektors (PSI), die weiterverwendet werden sollen, personenbezogene Daten enthalten. Statt personenbezogenen Daten sind es oft die aus personenbezogenen Daten abgeleiteten statistischen Daten, die für die Weiterverwendung bereitgestellt werden und auch bereitgestellt werden sollten.

Dennoch ist es in einigen Situationen unter Umständen auch möglich, dass personenbezogene Daten nach den Bestimmungen der PSI-Richtlinie gegebenenfalls als für die Weiterverwendung zugänglich gelten, und zwar nach Maßgabe zusätzlicher rechtlicher, technischer oder organisatorischer Maßnahmen zum Schutz der betreffenden natürlichen Personen. Für diese Fälle wiederholt die Datenschutzgruppe, wie wichtig die Schaffung einer verbindlichen Rechtsgrundlage für die öffentliche Bereitstellung personenbezogener Daten ist, wobei die einschlägigen Datenschutzvorschriften zu berücksichtigen sind, einschließlich der Grundsätze der Verhältnismäßigkeit, der Datensparsamkeit und der Zweckbindung. In diesem Zusammenhang ist unbedingt nochmals darauf hinzuweisen, dass alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, unabhängig davon, ob sie öffentlich verfügbar sind oder nicht, personenbezogene Daten darstellen. Daher fallen der Zugang zu öffentlich bereitgestellten personenbezogenen Daten und deren Weiterverwendung nach wie vor unter das geltende Datenschutzrecht.

Angesichts dieser Erwägungen empfiehlt die Artikel-29-Datenschutzgruppe Folgendes:

- Die Tatsache, dass einige Informationen des öffentlichen Sektors (PSI) personenbezogene Daten enthalten können, sollte schon im ersten Moment berücksichtigt werden, in dem darüber nachgedacht wird, Informationen des öffentlichen Sektors öffentlich zugänglich zu machen und dabei die Grundsätze der Berücksichtigung des Datenschutzes bereits in der Planungs- und Entwicklungsphase ('data protection by design') wie auch im Fall von bestehenden Verarbeitungssystemen seiner Berücksichtigung nach Maßgabe der datensparsamsten Voreinstellungen ('data protection by default') zu verfolgen’.
- In diesem Sinne sollte die betreffende öffentliche Stelle (bzw. der Gesetzgeber) eine Datenschutz-Folgenabschätzung durchführen, bevor eine Information des öffentlichen Sektors, die personenbezogene Daten enthält, zu Zwecken der Weiterverwendung zugänglich gemacht werden kann (oder bevor ein Gesetz verabschiedet wird, das die Veröffentlichung personenbezogener Daten gestattet und sie somit für die Weiterverwendung potenziell zugänglich macht); eine Datenschutz-Folgenabschätzung sollte auch in Situationen durchgeführt werden in denen anonymisierte Datensätze, die aus personenbezogenen Daten abgeleitet wurden, zu Zwecken der Weiterverwendung bereitgestellt werden.
- Wenn Datensätze anonymisiert werden, ist es von großer Bedeutung, das Rückidentifizierungsrisiko zu bewerten, und eine bewährte Verfahrensweise, die Rückidentifizierung einem Testdurchlauf zu unterziehen.

- Das Ergebnis der Bewertung könnte dabei behilflich sein, die geeigneten Sicherheits- und Schutzmaßnahmen zur Risikominimierung zu ermitteln; dazu gehören ohne jede Begrenzung auch die rechtlichen, technischen und organisatorischen Maßnahmen, wie z. B. angemessene Lizenzbedingungen und technische Maßnahmen zur Verhinderung von Massen-Downloads von Daten sowie geeignete Anonymisierungstechniken; es kann auch zu der Entscheidung führen, von der Veröffentlichung und/oder der Bereitstellung zu Zwecken der Weiterverwendung abzusehen.
- Die Lizenzbedingungen zur Weiterverwendung von Informationen des öffentlichen Sektors (PSI) sollten eine Datenschutzklausel umfassen, wenn personenbezogene Daten verarbeitet werden, die auch auf Situationen eingeht, in denen anonymisierte Datensätze, die aus personenbezogenen Daten abgeleitet wurden ,zu Zwecken der Weiterverwendung bereitgestellt werden.
- Kommt die Datenschutz-Folgenabschätzung zu dem Ergebnis, dass eine offene Lizenz nicht ausreicht, um auf die Datenschutzrisiken einzugehen, sollten die öffentlichen Stellen keine personenbezogenen Daten im Rahmen der PSI-Richtlinie bereitstellen. (Jedoch kann die öffentliche Stelle immer noch nach ihrem Ermessen eine Weiterverwendung außerhalb des Anwendungsbereichs und der Bedingungen der PSI-Richtlinie in Betracht ziehen und von den Antragstellern verlangen, darzulegen, dass auf alle Risiken für den Schutz personenbezogener Daten angemessen eingegangen wird, und dass der Antragsteller die Daten gemäß dem einschlägigen Datenschutzrecht verarbeiten wird).
- Die öffentlichen Stellen sollten gegebenenfalls sicherstellen, dass personenbezogene Daten anonymisiert werden und die Lizenzbedingungen die Rückidentifizierung von natürlichen Personen sowie die Weiterverwendung von personenbezogenen Daten zu Zwecken, die die betroffenen Personen beeinträchtigen können, speziell verbieten.
- Schließlich sollten die Mitgliedstaaten auch in Betracht ziehen, Fördermaßnahmen für Wissensnetze/Kompetenzzentren auf die Beine zu stellen und diesen zu gewähren und damit den Austausch und die gemeinsame Nutzung bewährter Praktiken im Zusammenhang mit Anonymisierung und Offenen Daten zu ermöglichen.

Brüssel, den 5. Juni 2013

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM