März 2017 · Julia Manske und Dr. Tobias Knobloch

Leitfaden für Datenschutz bei Open Data

Ansätze und Instrumente für die verantwortungsvolle Öffnung von Verwaltungsdaten

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Mit der bevorstehenden Verabschiedung des Open-Data-Gesetzes öffnet Deutschland erstmals großflächig seine Verwaltungsdaten. Damit macht die Bundesrepublik es Ländern wie Frankreich, Großbritannien und Kanada nach und schafft endlich eine wichtige Grundlage für soziale und wirtschaftliche Innovationen. Ein wichtiger Schritt ist damit getan.

Die nächste Herausforderung besteht darin, bei der Öffnung von Regierungs- und Verwaltungsdaten verantwortungsbewusst vorzugehen. In Deutschland herrscht eine hohe Datenschutzsensibilität und ein starkes öffentliches Interesse am Schutz der Privatsphäre. In einer Zeit stetiger Datafizierung, automatisierter Verarbeitung und der Verbreitung datengetriebener Geschäftsmodelle reicht deshalb ein rein juristischer Blick auf den Datenschutz nicht aus, um den Schutz der Bürger zu gewährleisten.

Für dieses Problem gibt es Lösungen. Mit Blick auf die bevorstehende Verabschiedung des Open-Data-Gesetzes und die danach anstehende Umsetzung liefert der vorliegende Leitfaden im ersten Teil sechs generelle Empfehlungen, welche Rahmenbedingungen zum Schutz von Grundrechten geschaffen werden sollten. Der zweite Teil bietet ab Seite 16 einen Werkzeugkasten, der konkrete Vorschläge macht, wie Prozesse vor, während und nach der Datenöffnung zu gestalten sind und welche Instrumente angewendet werden können, um Datenschutzrisiken angemessen zu berücksichtigen.

Beispielsweise schlagen wir ein Bewertungsverfahren von Daten in Anlehnung an ein Ampelsystem vor, ähnlich wie es in der Stadt San Francisco bereits zur Anwendung kommt. Um die Qualität von Anonymisierungsverfahren im Zuge der Öffnung von Daten zu erhöhen, empfehlen wir ferner, Behördenmitarbeiter im Umgang mit Anonymisierungsverfahren zu schulen, auf technische Hilfestellungen zurückzugreifen und die Art der Anonymisierung als Metadaten zu verzeichnen. Außerdem plädieren wir für restriktive Zugangssysteme zu bestimmten Datensätzen, die besonders wertvoll, aber auch hoch sensibel sind. Ein weiterer Vorschlag bezieht sich auf kontinuierliche “Stresstests”, etwa durch externe Experten, die das Risiko einer De-Anonymisierung von Datensätzen unter Zuhilfenahme anderer Datensätze zu prüfen hätten. Hier lässt sich von der IT-Sicherheit lernen.

Diese und weitere Instrumente werden mit Beispielen aus dem Ausland und aus anderen Arbeitsfeldern angereichert. Auch werden ihre Chancen und Risiken diskutiert, um Behördenmitarbeitern und Open-Data-Interessierten ein umfangreiches Repertoire, um Daten zu öffnen und die Risiken minimiert, an die Hand zu geben.

Inhaltsverzeichnis

Die Autoren bedanken sich bei den Teilnehmern des Workshops „Open Data & Privacy“ am 28.11.2016 sowie bei Dr. Roland Goetzke, Jan Schallaböck, Sven Hense, Prof. Ulrich Greveler für ihre wertvollen Beiträge und Anmerkungen. Außerdem danken wir dem Team der Stiftung Neue Verantwortung für die Unterstützung, insbesondere Leonie Beining.

Kontextualisierung und sechs grundsätzliche Empfehlungen

Offene Verwaltungsdaten[1] sind inzwischen fester Bestandteil der Digitalisierungsstrategie der Bundesregierung. Sie bilden ein wesentliches Puzzlestück eines Datenökosystems, das Quelle einer Vielzahl gesellschaftlicher Innovationen sein kann.[2] Genutzt werden sie von der Verwaltung selbst, von Wissenschaft, Politik, Zivilgesellschaft, Start-ups und etablierten Unternehmen. Dabei potenzieren sich die Möglichkeiten, wenn offene Verwaltungsdaten mit Daten anderer Quellen kombiniert werden. Daraus folgt aber auch, dass sie, ebenso wie Daten anderen Ursprungs, etwa aus der Privatwirtschaft, Teil des Big-Data-Kosmos werden und zu den Herausforderungen beitragen, die in diesem Kontext aktuell diskutiert werden. An erster Stelle betrifft das den Schutz der Privatsphäre. Wie aktuelle Beispiele zeigen, können die gesellschaftlichen Implikationen einer Datennutzung aber weit über den klassischen Datenschutz hinausgehen, beispielsweise wenn dadurch Diskriminierungen verstärkt werden.[3] Internationale Beispiele zeigen, dass auch offene Verwaltungsdaten zu diesen Problematiken beitragen können.[4]

In unserem Papier „Offene Daten und der Schutz der Privatsphäre“ (Oktober 2016) haben wir die Herausforderungen, die mit der Öffnung von Verwaltungsdaten verbunden sind, wie folgt klassifiziert:

1. Daten werden aus falschen oder intransparenten Gründen geöffnet beziehungsweise von der Öffnung ausgeschlossen.[5]

1 Offene Daten zeichnen sich dadurch aus, dass sie von jedermann und für jegliche Zwecke genutzt, (maschinell) weiterverarbeitet und weiterverbreitet werden können. In diesem Papier beziehen wir uns auf offene Verwaltungs- und Regierungsdaten, wie etwa Umwelt- und Wetterdaten, Geodaten, Verkehrsdaten, Gesundheitsdaten, Haushaltsdaten, Statistiken, Publikationen, Protokolle, Gesetze, Urteile und Verordnungen.

2 Knobloch, T.; Manske, J. (2016). Das Datenzeitalter gestalten. Offene Verwaltungsdaten sind der Schlüssel. https://www.stiftung-nv.de/de/publikation/das-datenzeitalter-gestalten, vgl. auch www.datenwirken.de.

3 Siehe exemplarisch O’Neil, C. (2016): Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, New York.

4 Manske, J. (2016). Offene Daten und der Schutz der Privatsphäre. https://www.stiftung-nv.de/de/publikation/offene-daten-und-der-schutz-der-privatsphaere.

5 Wir möchten an dieser Stelle noch einmal betonen, dass wir uns explizit auf den Schutz der Privatsphäre und der informationellen Selbstbestimmung der Bürger konzentrieren. Datenschutz darf hingegen nicht als Vorwand missbraucht werden, Daten, die beispielsweise der Transparenz staatlichen Handelns dienen, nicht öffentlich zugänglich zu machen. Dies ist in der Vergangenheit im Rahmen des Informationsfreiheitsgesetzes geschehen. Gleichzeitig bringen offene Daten aber Probleme mit sich bringen, die über die im Informationsfreiheitsgesetz geregelten Fälle hinausgehen, wie wir im Papier von Oktober erläutert haben, vgl.: Manske (2016), S. 11 f.

2. Daten werden falsch geöffnet, etwa indem qualitativ schlechte Anonymisierungsverfahren zur Anwendung kommen.
3. Anonymisierte Daten können durch Verknüpfung mit anderen – gegebenenfalls ebenfalls öffentlich verfügbaren – Datenquellen deanonymisiert werden

4. Offene Verwaltungsdaten werden für Zwecke genutzt, die rechtswidrig oder von der Öffentlichkeit als unethisch bewertet werden.

Die deutsche Bundesregierung befindet sich mit der Verabschiedung eines Open-Data-Gesetzes aktuell auf einem guten Weg, mittelfristig umfassend Verwaltungsdaten in Deutschland bereitzustellen. Umso wichtiger wird es daher sein, von Anfang an die richtigen Rahmenbedingungen zu schaffen, um zu verhindern, dass die Grundrechte von Bürgern eingeschränkt oder offene Daten etwa für dubiose Geschäftsmodelle oder zum Zwecke der Profilbildung missbraucht werden. Denn ganz unabhängig von der rechtlichen Dimension wird auch das Vertrauen der Bürger über den langfristigen Erfolg offener Daten entscheiden. Auch wenn momentan politische Stimmen lauter werden, die sich gegen einen starken Datenschutz aussprechen6, sind wir der Überzeugung, dass gerade in Deutschland günstige Voraussetzungen herrschen, um die Öffnung von Verwaltungsdaten verantwortungsvoll und im Einklang mit bürgerlichen Grundrechten zu gestalten.

Als Grundlage dafür haben wir in unserem Papier vom letzten Oktober fünf Empfehlungen skizziert. Der erste dort genannte Punkt betrifft die Einführung klarer und transparenter Standards und Prinzipien zur Abwägung, ob Daten geöffnet werden sollen. Dies ist auch deshalb so wichtig, um zu verhindern, dass der Datenschutz als Vorwand genutzt wird, gesellschaftlich relevante Daten, die etwa Transparenz über staatliches Handeln erzeugen, nicht zu öffnen. Zweitens müssen die Anforderungen der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) bei der Umsetzung einer Open-Data-Strategie berücksichtigt werden. Drittens sind Standards und Kompetenzaufbau für die Anonymisierung von Datensätzen erforderlich. Viertens darf dabei nicht ignoriert werden, dass die Forschung inzwischen die Grenzen der Anonymisierung von Daten belegt, sodass diese Maßnahme allein nicht ausreichen wird, um den Schutz der Privatsphäre zu gewährleisten. Fünftens müssen offene Daten als Teil des allgemeinen Diskurses über die verantwortungsvolle Datennutzung verstanden und insofern bei der Betrachtung der Chancen und Risiken von Daten im Allgemeinen berücksichtigt werden.

6 Vgl. etwa die Rede von Bundeskanzlerin Angela Merkel anlässlich des IT-Gipfels 2016 über die aus ihrer Sicht notwendige Abschwächung des Datenschutzes zugunsten von Geschäftsmodellen: http://www.handelsblatt.com/impressum/nutzungshinweise/blocker/?callback=%2Fpolitik%2Fdeutschland%2Fdigitalisierung-angela-merkel-will-den-datenschutz-lockern%2F14859824.html.

Diese generellen Vorschläge gilt es nun mit konkreten Prozessen und Instrumenten zu unterlegen. Diesem Zweck dient das vorliegende Dokument. Viele der hier versammelten Ansätze stammen aus dem Ausland oder sind inspiriert von Verfahren in benachbarten Bereichen, zum Beispiel der IT-Sicherheit. Eine erste Version dieser Instrumentensammlung wurde in einem Workshop im November 2016[7] mit Experten aus Verwaltung, Datenschutz, IT und Zivilgesellschaft sowie in Einzelgesprächen mit weiteren Experten evaluiert und fortlaufend verfeinert.

Die Ansätze orientieren sich an drei Prozessphasen offener Verwaltungsdaten:

1. Vor der Veröffentlichung
2. Bei der Veröffentlichung
3. Nach der Veröffentlichung[8]

Die Darstellung der konkreten Instrumente mit der Diskussion der jeweils verbundenen Chancen und Risiken sowie Verweise auf Beispiele aus anderen Bereichen oder Ländern finden sich in der Tabelle ab Seite 16. Die Beschreibung des Prozessablaufes jeweils am Anfang der drei skizzierten Phasen soll konkretisieren, wie die Umsetzung der Instrumente in der Praxis aussehen könnte. Auf Basis unserer Recherche und intensiver Dialoge an der Schnittstelle offene Daten und Datenschutz möchten wir überdies die folgenden sechs grundsätzlichen Empfehlungen für eine starke Berücksichtigung von Datenschutzaspekten bei der Bereitstellung offener Daten aussprechen:

1. Mehr als einen Haken setzen: Kapazitätsaufbau und Ressourcen

Wir möchten dazu ermuntern, Verwaltungsmitarbeitern eine ganzheitliche Perspektive auf den Nutzen und die Risiken offener Daten zu vermitteln. Solange Datenschutz nur als eine Checkbox betrachtet wird, die es juristisch abzuhaken gilt, nicht jedoch strategisch in Prozesse integriert wird, erhöht sich die Gefahr, dass Datenöffnung eher dazu beiträgt, gesellschaftliche Probleme zu verursachen, anstatt sie zu lösen.

Dies ist weniger aufwendig, als es klingt, schließlich muss die Verwaltung

7 Hinweis zur Veranstaltung: https://www.stiftung-nv.de/veranstaltung/open-data-privacy-workshop.

8 Dies ist natürlich eine Verkürzung, genau genommen handelt es sich eher um einen „Lebenszyklus“ von Daten. Altman et al. unterteilen etwa in fünf Phasen: Sammlung, Verarbeitung, Speicherung, Öffnung und Nutzung. Altman, M; Wood, A.; O‘Brien, D.; Vadhan, S.; Gasser, U. (2016). Towards a Modern Approach to Privacy-Aware Government Data Releases. In: Berkeley Technology Law Journal, 30 (3), S. 1968–2072. http://openscholar.mit.edu/sites/default/files/dept/files/modernopendataprivacy.pdf.

für Open Data ohnehin Kapazitätsaufbau betreiben. Dafür werden so oder so Ressourcen benötigt. Wir plädieren dafür, dass dabei auch der Aufbau von Kapazitäten für den Schutz der Privatsphäre berücksichtigt und in die Ressourcenplanung mit einbezogen wird.

Erfreulicherweise sieht der Open-Data-Gesetzesentwurf den Aufbau einer Open-Data-Beratungsstelle vor, die voraussichtlich zunächst mit sechs und später mit vier Stellen ausgestattet sein soll.[9] Aus unserer Sicht wäre es eine verpasste Chance, wenn in dieser Beratungsstelle keine Kompetenzen für die Risikoanalyse von Daten sowie für den technischen Datenschutz angesiedelt würden. Schließlich sind spezielle Kenntnisse erforderlich, um sowohl Chancen als auch Gefahren adäquat erkennen und beurteilen zu können. Das Generalistenprinzip gerät hier an eine Grenze, die von den technischen Entwicklungen des Datenzeitalters gezogen wird.

Möglichst kurzfristig sollten Leitfäden und Checklisten für das Auffinden, Einstufen, Aufbereiten und Veröffentlichen von Datensätzen bereitgestellt werden. Diese Materialien stellen eine erste wichtige und vor allem niedrigschwellige Hilfestellung für Behördenmitarbeiter dar. Allerdings werden sie nicht ausreichen, um potenzielle Risiken von Daten in Gänze abschätzen zu können. Vielmehr müssen Verwaltungsmitarbeiter in professionellen Trainings geschult werden. Dies könnte beispielsweise in ein umfassenderes Datenkompetenz-Training, von dem die Mitarbeiter und ihre Dienststellen auch sonst sehr profitieren würden, integriert werden. Ähnlich wie es der Government Digital Service in Großbritannien vorlebt[10], erscheinen integrierte Lernansätze (Blended Learning), die sowohl aus E-Learning-Angeboten als auch auf Präsenzveranstaltungen basieren, dafür als vielversprechend.

Dass eine gute digitale Infrastruktur innerhalb der Behörden, wie entsprechende Software oder digitale Schnittstellen, die Datenöffnung erleichtert, wurde mehrfach betont.[11] Umso erfreulicher ist es, dass das Open-Data-Gesetz des Bundes unter dem Stichwort „open by design“ explizit dazu ver-

9 Vgl. Entwurf eines Ersten Gesetzes zur Änderung des E-Government-Gesetzes, Stand 13.01.2017, Absatz 10 sowie die Formulierung zum Erfüllungsaufwand für die Verwaltung auf S. 4: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/entwurf-open-data-gesetz.pdf?__blob=publicationFile.

10 Erste Ausführung dazu: https://gds.blog.gov.uk/2016/04/27/data-literacy-helping-non-data-specialists-make-the-most-of-data-science.

11 Vgl. z.B. The Potsdam Institute for eGovernment / BMI (2015). Auswirkungen der Abgabe von Daten gegen Geldleistungen in der Verwaltung unter besonderer Berücksichtigung der Bundesverwaltung, S. 57. https://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/2016/entgeltstudie-open-data.html; Janssen, M.; Charalabidis, Y.; Zuiderwijk, A. (2012). Benefits, Adoption Barriers and Myths of Open Data and Open Government. Information Systems Management, 29 (4), S. 258–268. http://doi.org/10.1080/10580530.2012.716740.

pflichtet, bei jeder Veränderung elektronischer Verwaltungsprozesse die Bereitstellung offener Daten auf technischer Ebene zu berücksichtigen und so den Arbeitsaufwand für die Öffnung von Daten deutlich zu verringern. Tatsächlich begünstigt eine solche Open-Data-freundliche Infrastruktur auch den Schutz der Daten, da die Steuerung und Standardisierung von Prozessen rund um die Daten vereinfacht wird und so ein besserer Überblick über die Daten geschaffen wird. Dies wiederum erleichtert es, Fehler zu finden beziehungsweise zu vermeiden.

2. Risikoanalyse der Daten

Je besser das Wissen über öffnende beziehungsweise bereits geöffnete Daten ist, desto leichter lässt sich das möglicherweise von ihnen ausgehende Risiko abschätzen. Insofern sollten Datensätze standardmäßig einer Kategorisierung unterzogen werden.[12] Das erleichtert die Risikofolgenabschätzung, wie sie in Phase vor der Datenveröffentlichung zu erfolgen hat. Die bereits erwähnten Checklisten könnten dazu dienen, Daten anhand eines Ampelsystems zu kategorisieren. „Rote Daten" dürften zunächst generell gar nicht geöffnet werden, „grüne" dagegen, die eindeutig und auch mit größter Wahrscheinlichkeit zukünftig keinen Personenbezug aufweisen, könnten problemlos bereitgestellt werden. Die Einstufung müsste bei den datenhaltenden und -bearbeitenden Stellen vorgenommen werden, da sie die Daten am besten kennen. Dabei muss das Vier-Augen-Prinzip gelten. Einmal etabliert, kann eine solche Kategorisierung zu einer schnellen Entscheidung über die Öffnung von Daten führen.

Ein besonderes Augenmerk – und potenzieller Mehraufwand – läge lediglich auf der Prüfung der „orangen Daten". Spätestens für diese Datensätze muss beim Vier-Augen-Prinzip der fachlich Zuständige durch jemanden mit Datenschutzexpertise ergänzt werden. Zu unserer Überraschung sprachen sich mehrere Verwaltungsmitarbeiter sogar für die Etablierung einer vermittelnden Stelle mit entsprechender Expertise aus („Clearing-Stelle" für Datenschutzbelange bei der Öffnung von Verwaltungsdaten). Eine solche Funktion könnte zum Beispiel von der Open-Data-Beratungsstelle ausgeübt werden. Zu beachten gilt, dass themenspezifische, anwendungsfeldbezogene Ansätze dabei unverzichtbar sein werden, da die Datensätze bestimmter Arbeitsbereiche tendenziell ein höheres Risiko mit sich bringen – etwa im Geo- und Gesundheitsdatenbereich.

Obwohl die Bewertung einzelner Datensätze an und für sich wichtig ist, wird dies für eine solide Einschätzung möglicher Risiken nicht ausreichen. Dazu müssen die singulären Daten immer in Verbindung mit anderen Datensätzen betrachtet werden. Zudem gilt einmal mehr, dass die Risiken, die von Daten

12 Sicherlich würde auch eine Katalogisierung der Datensätze zur Abschätzung der Datenschutzrisiken hilfreich sein, mit der breiten Öffnung von Daten wäre dieser Ansatz aber langfristig zu aufwendig und nur schwer durchführbar.

ausgehen, dynamisch sind. Das wiederum bedeutet, dass auch jede Kategorisierung regelmäßigen Prüfungen unterzogen werden muss. Einerseits, weil das Risiko mit den Daten wächst, und andererseits, weil die Definition dessen, was gesellschaftlich relevant oder aber sensibel ist, kontinuierlichen Aushandlungsprozessen unterliegt. Dies zeigt sich zum einen am Beispiel der zunehmenden Veröffentlichung von vormals unter Verschluss stehenden ÖPNV-Datenbeständen, und zum anderen in der nun eingekehrten Zurückhaltung bei der Veröffentlichung von Daten von Flüchtlingseinrichtungen oder kritischen Infrastrukturdaten wie Leitungsnetze von Energieversorgern. Auf den Aspekt der kontinuierlichen Prüfung kommen wir unten noch einmal zurück.

3. Ohne qualitativ hochwertigen technischen Datenschutz geht es nicht

Qualitativ hochwertige technische Datenschutzverfahren spielen bei der verantwortungsvollen Öffnung von Daten eine zentrale Rolle – umso mehr, wenn wir über eine breitflächige Datenbereitstellung sprechen. Die momentane Diskrepanz zwischen der technischen und der rechtlichen Bewertung von Datenschutz ist bedenklich. Das Open-Data-Gesetz spricht sich explizit für die Öffnung aller Daten aus, die per Definition keine personenbezogenen Daten sind und nicht aus anderen, in bereits bestehenden Informationszugangsgesetzen definierten Gründen (zum Beispiel Geheimschutz) geschützt werden müssen. Dies bedeutet, dass auch anonymisierte Datensätze – also jene, in denen Personenbezüge zuvor enthalten waren und dann entfernt wurden – geöffnet werden sollen. Ein Jurist würde der Veröffentlichung anonymisierter Datensätze daher stets zustimmen. Doch die Rechtmäßigkeit ist noch kein Garant für einen verantwortungsvollen Umgang mit den so geöffneten Daten. Und Anonymisierung ist nicht gleich Anonymisierung, auch wenn es für den Laien so erscheinen mag. In diesem Zusammenhang ist es zu beklagen, dass im Open-Data-Gesetz keine Aussage dazu getroffen wird, welche Stelle für die Anonymisierung von Datensätzen zuständig ist.

Der Umfang einer Anonymisierung und das dadurch erreichte Sicherheitsniveau können sehr unterschiedlich ausfallen. Problematisch an der Situation in Deutschland ist, dass unterschiedliche Standards für die Anonymisierung, etwa bezüglich des Aggregationslevels von Daten, gelten. Kommunen und Länder schätzen das Datenschutzrisiko unterschiedlich ein. Wünschenswert wäre eine Harmonisierung der rechtlichen Interpretationen durch die Landesdatenschutzbeauftragten. Denn ohnehin stellt sich eine qualitativ hochwertige Anonymisierung von Daten angesichts der rasant schnellen, automatisierten Verarbeitung großer Datenmengen als sehr schwierig dar. Zahlreiche Forschungen weisen sogar darauf hin, dass eine vollständige und dauerhaft wirksame Anonymisierung nach aktuellem Stand der Technik gar

nicht gewährleistet werden kann.[13] Man kann also allenfalls von einer Annäherung an ein hohes Datenschutzniveau, nicht aber von einem Garanten sprechen. Diese Erkenntnisse zu ignorieren, darf bei der Entwicklung und Umsetzung von Open-Data-Strategien der unterschiedlichen Verwaltungsebenen in unseren Augen keine Option sein.

Dies bedeutet nicht, dass Anonymisierung als Verfahren aufgegeben werden sollte. Vielmehr ist sie, sofern vollumfassend und von hoher Qualität, als ein notwendiges, aber eben nicht ausreichendes Element zu betrachten. Um einen hohen Qualitätsstandard zu erreichen, müssen entsprechende Strukturen geschaffen werden. Der dafür erforderliche Aufwand ist dabei nicht zu unterschätzen. Zum einen bedarf es, wie bereits erwähnt, des Kapazitätsaufbaus innerhalb der Verwaltung. Konkret: Um der Komplexität heutiger Anonymisierungsverfahren gerecht zu werden, müssen Verwaltungsmitarbeiter geschult werden. Zum anderen sollte gleichzeitig, wenn tatsächlich an einem guten Datenschutz gelegen ist, nicht allein der juristische Blick auf die Daten erfolgen, vielmehr muss grundsätzlich eine technische Betrachtungsweise mit einfließen.

Bislang ist bei Behördenmitarbeitern eher eine ablehnende Haltung gegenüber Ansätzen des technischen Datenschutzes zu erkennen. Natürlich kann es keine Lösung sein, sich ausschließlich auf technische Verfahren zu verlassen. Entsprechende unterstützende Tools könnten die Arbeit der Behörden allerdings deutlich erleichtern und Fehler minimieren; insbesondere dann, wenn sie in Fachverfahren integriert werden würden. Bisherige Angebote mögen dafür noch nicht infrage kommen; umso wünschenswerter wäre es, wenn in die Entwicklung nutzerfreundlicher Anwendungen auf Basis existierender Technologien speziell für die Bereitstellung offener Daten durch Behörden investiert würde.

4. Durchführung regelmäßiger Risikoprüfungen

Wie auch in allen anderen Bereichen, in denen mit Daten umgegangen wird, gilt es, Datenschutz als Prozess und nicht als eine einmalige Prüfung zu verstehen. Das muss sich natürlich auch in Budgets und der Ressourcenplanung abbilden. Angesichts der rapiden technologischen Veränderungen kann sich das Risiko der Verletzung der Privatsphäre innerhalb kurzer Zeit deutlich erhöhen. Gleichzeitig ist es aber auch möglich, dass neue technische Lösungen entwickelt werden, die Daten besser schützen. Nicht zuletzt die EU-DSGVO wird die Forschung und Entwicklung im Bereich datenschutz-

13 Ohm, P. (2009/2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. In: UCLA Law Review, 57, S. 1701–1777, U of Colorado Law Legal Studies Research Paper 9–12. http://ssrn.com/abstract=1450006; de Montjoye Y.-A.; Radaelli, L.; Singh, V. K.; Pentland, A. S. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. In: Science, 347 (6221), S. 536–539. DOI:10.1126/science.1256297.

freundlicher Technologien (Privacy Enhancing Technology, PET)[14] vorantreiben.

Insofern müssen mögliche Datenschutzrisiken fortlaufend geprüft werden. Bei solchen „Anonymisierungsstresstests" sollten zunächst Aktualität und Qualität der Anonymisierungsverfahren beurteilt werden. Dann gilt es, den Blick auf das gesamte Datenökosystem und nicht etwa nur auf singuläre Datensätze zu richten. Anleitende Fragen für eine entsprechende Prüfunge wären etwa:

- Welche Überschneidungen gibt es zwischen den Datensätzen auf der Datenplattform und welche Rückschlüsse sind dadurch möglich?

- Welche Verschneidungen ergeben sich aus dem Heranziehen offener Verwaltungsdaten aus anderen Plattformen (etwa auf kommunaler Ebene)?

- Welche Daten lassen sich gegebenenfalls durch das Heranziehen anderer (zum Beispiel kommerzieller) Datensätze leichter deanonymisieren?

Stichprobenartig sollte so turnusmäßig kontrolliert werden, ob und warum die Gefahr einer Deanonymisierung besteht. Wir regen an, dafür die Entwicklung entsprechender technisch unterstützender Instrumente zu fördern und zu prüfen, ob und inwieweit sie sich in Fachanwendungen integrieren lassen. Im Zuge der gesetzlich vorgeschriebenen Open-Data-Fähigkeit neu anzuschaffender Informationsverarbeitungssysteme muss der technische Datenschutzanspekt ausreichend berücksichtigt werden.

In regelmäßigen Abständen würde es sich außerdem anbieten, eine Risikoprüfung an ein externes Audit mit entsprechend ausgereifter technischer Expertise zu vergeben. Hier ist zu diskutieren, wer diese Aufgabe übernehmen sollte. Der Aufgabenbereich der – ohnehin ressourcenarmen – unabhängigen Datenschutzbehörden ist auf Beratung begrenzt. Anregung könnten aber etablierte Verfahren aus dem Bereich der IT-Sicherheit bieten. Dort führen externe Hacker geplant Penetrationstests durch, um die Sicherheit der Systeme zu prüfen (man spricht auch von „Bug-Bounty-Programmen"). In Deutschland bietet dies etwa der Chaos Computer Club an.

Um dynamischer auf Fehler reagieren zu können und aus ihnen rechtzeitig zu lernen, hilft es, Fälle aus dem In- und Ausland zu betrachten und auszu-

14 Siehe hierzu auch den Bericht der European Union Agency for Network and Information Security, ENISA (2015). Privacy by design in big data. https://www.enisa.europa.eu/publications/big-data-protection.

werten. Natürlich sind viele Beispiele aus anderen Ländern allein aufgrund der unterschiedlichen rechtlichen Rahmenbedingungen nicht auf Deutschland übertragbar, nichtsdestotrotz kann eine Systematisierung von Fehlern beziehungsweise Missbrauchsfällen (idealerweise inklusive der jeweils ausgehebelten Anonymisierungsart) eine Grundlage für die Bewertung von Daten bieten (siehe Ampelsystem) und die Kompetenzen innerhalb der Verwaltung erhöhen.

Überdies plädieren wir für mehr Transparenz hinsichtlich der Art der eingesetzten Anonymisierungsverfahren. Wie schon in unserem Papier vom vergangenen Herbst erwähnt, könnte dafür auf den Datenplattformen selbst über die angewandten Verfahren hingewiesen werden. Eine weitere Maßnahme, die aus Sicht des technischen Datenschutzes besonders zu begrüßen wäre, bestünde in der Dokumentation und Veröffentlichung des genutzten Anonymisierungsverfahrens in den Metadaten zum jeweiligen Datensatz.

5. Erwägung regulatorischer Ansätze

Auch wenn aus nachvollziehbaren Gründen vieles gegen regulatorische Ansätze spricht, möchten wir dennoch dafür plädieren, diese nicht grundsätzlich auszuschließen. Vermehrt erfahren wir, dass Daten für Cyberverbrechen missbraucht oder aber für Geschäftspraktiken genutzt werden, die aus einer Gemeinwohlperspektive unvertretbar sind (etwa wenn sozial Benachteiligten gezielt faule Kredite angeboten werden15). Hinter vielen dieser Praktiken stecken sogenannte Datenhändler. Natürlich stammen die meisten ihrer Daten aus kommerziellen Quellen, nichtsdestotrotz zeigt zumindest der Bericht der Federal Trade Commission aus den USA16 (zu Deutschland oder Europa liegen leider keine vergleichbaren Informationen vor), dass auch offene Verwaltungsdaten eine der Informationsquellen sind, derer sich die Händler bedienen. Immer mehr Fälle zeigen, dass hier auch anonymisierte Daten deanonymisiert und weiterverwendet werden. Deanonymisierte Daten können beispielsweise auch dazu verwendet werden, gezielte Betrugsangriffe auf Personen durchzuführen. Selbstverständlich haben offene Daten nur einen kleinen Anteil am grundsätzlichen Problem der Verletzung von Bürgerrechten durch die Analyse von Daten. Die Open-Data-Bewegung wird dieses Problem nicht lösen können. Vor dem Hintergrund aber, dass die Öffnung von Regierungsdaten eine am Gemeinwohl ausgerichtete Idee ist, sollten alle, die in diesem Bereich arbeiten, zu Lösungsansätzen beizutragen bemüht

15 Vgl. Christl, W.; Spiekermann, S. (2016). Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Facultas, Wien, S. 89 f., mit Bezug auf Astray, L. (2015). Online Lead Generation and Payday Loans. https://www.teamupturn.com/reports/2015/led-astray.

16 Federal Trade Commission (2014). Data Broker. A Call for Transparency and Accountability. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

sein und sich für eine Kultur des angemessenen Datenumgangs einsetzen. Regulierung ist dabei eines der möglichen Instrumente, das man nicht vorzeitig kategorisch ausschließen sollte.

Zwar sehen wir den Ansatz, den Akt der Deanonymisierung als Straftat zu erklären, wie es aktuell in Australien umgesetzt und in Neuseeland in Betracht gezogen wird[17], kritisch. Allerdings gäbe es noch andere Möglichkeiten zur Unterbindung von Missbrauch, etwa eine Sanktionierung des Handels oder der Nutzung deanonymisierter Daten; oder auch der Nutzung von Daten für bestimmte „nicht-gemeinwohlorientierte" Zwecke. Wenn uns an einer chancen- und rechtebasierten Datennutzung gelegen ist, benötigen wir sowohl für den Datenzugang als auch die Datennutzung differenziertere Ansätze. Das Thema Open Government Data ist eine gute Gelegenheit, um damit zu beginnen und sich beispielsweise zu überlegen, welchen Nutzergruppen man welche Arten der Datennutzung erlauben möchte.[18]

Natürlich erschwert die Dynamik globaler Datenflüsse die Durchsetzung nationaler Gesetze[19], doch auch in anderen Bereichen hat sich die Beschränkung der legalen Nutzungsmöglichkeiten von Daten als wirkungsvoll bewährt. Im Archivrecht etwa wird die Nutzung von personenbezogenen Informationsbeständen für die Forschung zugelassen mit der Auflage, dass diese nicht veröffentlicht werden dürfen.[20] Auch im Statistikrecht macht man sich regulatorische Ansätze zunutze.[21] Und selbst das bestehende Datenschutzrecht schränkt die Nutzung von Daten ohnehin in dem Sinne ein, dass bei öffentlichen Daten die weitere Verwendung nur zulässig ist, sofern das berechtigte Interesse eventuell betroffener Personen nicht unverhältnismäßig beeinträchtigt wird.

---

17 In Australien gilt mit der Anpassung des Privacy Act durch die Privacy Amendment (Re-identification Offence) Bill (2016) rückwirkend seit dem 29. September 2016 die Durchführung der Reidentifizierung öffentlicher Daten als Straftat. http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1047; siehe außerdem den Bericht des neuseeländischen Datenschutzbeauftragten (2017): Report to the Minister of Justice under Section 26 of the Privacy Act. Six Recommendations for Privacy Act Reform. https://privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-report-to-the-Minister-of-Justice-under-Section-26-of-the-Privacy-Act.pdf.

18 In der zweiten Jahreshälfte 2017 startet die Stiftung Neue Verantwortung das Projekt „Data Governance", das auch solche weitergehenden Fragen erörtert.

19 Wobei dies generell kein Ausschlusskriterium sein sollte, schließlich gilt dies generell für die Nutzung von Daten. Immerhin wird die EU-DSGVO bereits den europäischen Markt harmonisieren.

20 Vielen Dank an Dr. Alexander Dix für diese Anregung.

21 Siehe etwa § 21 des Bundesstatistikgesetzes zum Verbot der Reidentifizierung. So werden die Statistikgesetze von einigen Experten auch als „frühe Big-Data-Gesetze" betitelt, vgl. Dix, A. (2016). Datenschutz im Zeitalter von Big Data. Wie steht es um den Schutz der Privatsphäre? In: Stadtforschung und Statistik, 1, S. 59–64. https://www.eaid-berlin.de/wp-content/uploads/2016/05/StSt-1-2016_Dix.pdf.

In die Zukunft gedacht, gibt es auch auf einer technischen Ebene inzwischen Forschungsansätze, die sich der Entwicklung sogenannter „Sticky Policies“ widmen.[22] Mit diesen würden Datensätze unveränderlich so markiert, dass jede rechtswidrige Nutzung langfristig nachvollziehbar wäre. Auch beschränkte Zugänge, etwa für zertifizierte Forscher, zu bestimmten Datensätzen in Verbindung mit Lizenzen oder steuerbaren Schnittstellen23 sind dafür vielversprechend.

6. Vernetzung von Experten und Expertisen

Einmal mehr bedarf es der weiteren Vernetzung der Expertise mehrerer Disziplinen. Wie hier erläutert wurde, reicht es aus unserer Sicht nicht aus, ausschließlich juristisch auf die Datennutzung zu blicken. Zwar ist diese Betrachtung unbestritten schon aus einer Compliance-Perspektive unerlässlich. Doch um das Ziel einer gemeinwohlorientierten und verantwortungsvollen Datenöffnung zu verfolgen, möchten wir dringend dazu anregen, diese Perspektive zu erweitern. An erster Stelle sehen wir die stärkere Einbindung technischer Datenschutzexperten. An zweiter Stelle muss der Austausch zwischen Datenschützern (technisch und juristisch), Open-Data-Community und der Verwaltung intensiviert werden. Idealerweise wird dieser Kompetenzkern durch Expertise aus Bereichen ergänzt, die von offenen Daten profitieren beziehungsweise negativ von ihnen betroffen sein könnten (zum Beispiel Altenpflege, Flüchtlingsbetreuung, Aidsberatung etc.).

22 Pearson, S.; Casassa Mont, M. (2011). Sticky Policies: An Approach for Managing Privacy across Multiple Parties. https://documents.epfl.ch/users/a/ay/ayday/www/mini_project/Sticky%20Policies.pdf.

23 Das Fraunhofer IESE hat anwendungsreife technische Möglichkeiten der Datennutzungskontrolle für den Industriebereich entwickelt, vgl.: https://www.iese.fraunhofer.de/de/competencies/security/ind2uce-framework.html. Eine Übertragung solch avancierter Datennutzungskontrollmöglichkeiten würde bei der Datenbereitstellung die Berücksichtigung von gleichzeitig sehr interessanten wie sensiblen Daten erlauben. Freilich wäre hier nicht mehr von einem Open Data der reinen Lehre zu sprechen.

Fazit

Das Potenzial offener Verwaltungsdaten ist enorm. Dieses gilt es auszuschöpfen, allerdings in einer Weise, die auch auf lange Sicht das Vertrauen der Bürger garantiert und sie vor Gefährdungen schützt. Wohl kaum ein anderes Feld bietet sich besser an, einen gemeinwohlorientierten und verantwortungsvollen Umgang mit Daten vorzuleben. Niemandem nützt es am Ende, wenn der Staat durch seine Datenbereitstellung dazu beiträgt, dass Bürger zur Angriffsfläche für Datenmissbrauch oder fragwürdige Geschäftsmodelle werden. In einer Zeit, da sich Politiker mit der Datenerhebung auf digitalen Plattformen, mit Profilbildung, Wahlbeeinflussung durch „Fake News“ und dergleichen auseinandersetzen, dürfte dies eigentlich keiner gesonderten Erwähnung bedürfen. Tatsächlich aber fällt vielen das Verständnis für die Datenschutzrelevanz bei Open Data nach wie vor schwer.

Ziel dieses Papiers und der nachfolgenden Instrumentensammlung ist jedoch keineswegs, im übertragenen Sinne die Pferde scheu zu machen. Vielmehr möchten wir damit frühzeitig zu einem vorausschauenden und verantwortungsvollen Open-Data-Ansatz anregen. Da das momentane „Allheilmittel“ Anonymisierung nicht mehr voll verlässlich ist, sollten von Beginn an entsprechende Schutzmaßnahmen eingeführt werden. Gerade bei Open Data kann und sollte man hierbei auch technische Instrumente mit einbeziehen.

März 2017 · Julia Manske und Dr. Tobias Knobloch

Toolbox

Ansätze und Instrumente für die verantwortungsvolle Öffnung von Verwaltungsdaten

Stiftung
Neue
Verantwortung

Toolbox: Ansätze und Instrumente zum Schutz der Privatsphäre bei der Öffnung von Verwaltungsdaten

1. Definition von open by default

Open by default ist die standardmäßige Bereitstellung derjenigen Daten, die die Verwaltung bei der Erfüllung ihrer öffentlich-rechtlichen Aufgaben erhebt, und zwar standardisiert, in maschinenlesbarer Form und zur kostenlosen, uneingeschränkten Weiterverwendung (siehe Open-Definition).

2. Ausnahmen von open by default

A. Ausnahmen, die sich aus der geltenden Rechtslage ergeben können

Folgende gesetzliche Einschränkungen geben den Rahmen für potenzielle Ausnahmen der standardmäßigen Bereitstellung vor:

- **Datenschutzgesetz(e)** und (demnächst) das **Open-Data-Gesetz** des Bundes („Erstes Gesetz zur Änderung des E-Government-Gesetzes“)
- Einschränkungen der Weitergabe und Weiterverwendung von Informationen, wie sie im **Informationsfreiheitsgesetz (IFG)** und **Informationsweiterverwendungsgesetz (IWG)** geregelt sind
- Einschränkungen der Veröffentlichung und Nutzung von Informationen in bereits bestehenden **Spezialgesetzen**: Umweltinformationsgesetz, Geodatenzugangsgesetz, Verbraucherinformationsgesetz
- **Geheimschutz**: Verschlusssachen im Sinne des Sicherheitsüberprüfungsgesetzes
- **Betriebs- und Geschäftsgeheimnisse**
- Sonstige Geheimnisschutz-relevante Bereiche: Statistikgeheimnis, Steuergeheimnis, Sozialgeheimnis, Berufsgeheimnisse (z.B. Ärzte)
- **Schutz geistigen Eigentums**: Urheberrechtsgesetz, Markengesetz, Patentrecht

Ferner muss das Veröffentlichungsinteresse grundsätzlich mit folgenden zu schützenden Rechtsgütern abgewogen werden:

- personenbezogene und personenbeziehbare Daten
- öffentliche Belange und Rechtsdurchsetzung
- Ablauf von Verwaltungsverfahren und bevorstehende behördliche Maßnahmen
- Angaben und Mitteilungen öffentlicher Stellen des Bundes oder anderer Länder
- Schutz des behördlichen Entscheidungsbildungsprozesses

B. Ausnahmen von den Ausnahmen

Die unter A genannten Ausschlussgründe geben den Rahmen vor. Sie sind kein abschließender Ausschlussgrund, sondern lassen erstens im Zuge der Abwägung mit dem Veröffentlichungsinteresse Spielräume für Ausnahmen. Dabei darf die Entscheidung über Veröffentlichung nicht der subjektiven Beurteilung von Behördenmitarbeitern überlassen werden, sondern muss auf ausformulierten Normen und Prinzipien beruhen. Zweitens können Daten generell so aufbereitet werden, dass sie dennoch öffentlich bereitgestellt werden können. So sind zwar personenbezogene Daten grundsätzlich von der Öffnung ausgeschlossen, anonymisierte Daten, also Daten, denen der ursprüngliche Personenbezug entzogen wurde, können nach juristischer Betrachtung aber bereitgestellt werden.

C. Der Kreis der zu veröffentlichenden Daten muss zum Schutz der Privatsphäre gegebenenfalls weiter eingeschränkt werden

Auch wenn dies rechtlich legitim wäre, können nach unserer Einschätzung im Sinne eines verantwortungsvollen Open-Data-Ansatzes nicht alle Daten, die beim Negativabgleich (vgl. A) übrig bleiben beziehungsweise im Zuge der Einzelfallentscheidung als gegebenenfalls veröffentlichungsfähig ermittelt werden (vgl. B), gefahrlos als Open Data bereitgestellt werden, auch dann nicht, wenn sie anonymisiert werden. Dabei können aus unserer Sicht auch nicht bedenkenlos die Kriterien des IFG & IWG auf Open Data übertragen werden, da die Gefahren für die Privatsphäre durch die Veröffentlichung von Informationen als Open Data in aller Regel sehr viel größer sind als durch eine gezielte Herausgabe an bestimmte Personen oder Institutionen und die entsprechende Weiterverwendung. Dies ist in der Hauptsache auf zwei Ursachen zurückzuführen (vgl. dazu auch unser Papier „Offene Daten und der Schutz der Privatsphäre“ vom Oktober 2016 sowie die diese Instrumentensammlung begleitenden Ausführungen):

- Technische Grenzen von Anonymisierungsverfahren
- Neue Risiken, die sich aus der maschinellen Verarbeitung und Kombinierbarkeit mit anderen Datensätzen ergeben

Aus diesem Grund bedarf es entsprechender Instrumente, mit denen mögliche Datenschutzrisiken durch offene Daten im Vorhinein abgeschätzt und im Zuge der Veröffentlichung minimiert werden können. Die Vorschläge und Ideen in dieser Übersicht dienen diesem Zweck.

3. Vorschlag eines Drei-Phasen-Modells zur Risikoabschätzung für Open Data

Nachfolgend unterscheiden wir diese drei Prozessphasen der Datenöffnung und schlagen für die jeweilige Phase Datenschutzmaßnahmen vor:

1. **Vor der Veröffentlichung:** Entscheidung, ob Daten überhaupt geöffnet werden dürfen beziehungsweise sollten
2. **Bei der Veröffentlichung:** Datenschutzmaßnahmen im Zuge der Veröffentlichung von Daten
3. **Nach der Veröffentlichung:** Steuerung der Nutzung bereits geöffneter Daten

Sämtliche Maßnahmen bauen natürlich auf laufenden Geschäftsprozessen auf, in denen Datenschutzprinzipien – wie Datenvermeidung und Datensparsamkeit, etwa bei der Beschaffung von IT-System – ohnehin verankert sind.

Die unterschiedlichen Maßnahmearten werden nachfolgend wie folgt unterschieden und benannt:

- **Bewertungshilfe**: Hilfen zur Bewertung des Datenschutzrisikos eines oder mehrerer Datensätze
- **Institutionalisierung**: Schaffung oder Nutzung von Institutionen oder institutionalisierten Prozessen
- **Kapazitätsaufbau**: Maßnahmen zur Sensibilisierung und Fortbildung der beteiligten Mitarbeiter und zur Entwicklung von Verfahren / Methoden
- **Technischer Datenschutz**: Bereitstellung technischer Infrastruktur für erhöhten Datenschutz
- **Regulierungsansatz**: stark reglementierende Maßnahmen der Verwaltung / des Gesetzgebers

Zudem sind diese in **kurzfristig (KF), mittelfristig (MF)** und **langfristig (LF)** umsetzbare Maßnahmen eingeteilt (siehe Abkürzung in der linken Spalte).

Wir teilen außerdem Daten in Anlehnung an ein **Ampelsystem** wie folgt ein:

Grün = Datensatz kann bedenkenlos als Rohdaten (nicht-anonymisiert) geöffnet werden
Orange = Datensätze müssen zunächst eine Prüfung durchlaufen und können ggf. unter Berücksichtigung bestimmter Schutzmaßnahmen geöffnet werden
Rot = Datensatz darf so auf keinen Fall geöffnet werden

Anmerkungen

Die im Folgenden vorgestellten Ansätze setzen auf sehr unterschiedlichen Ebenen an. Einige lassen sich sehr kurzfristig und niedrigschwellig umsetzen, während andere eher als Anregung für die Weiterentwicklung des Themas dienen. Die Vorschläge sind nicht isoliert, sondern als Elemente eines Baukastens zu betrachten. Grundsätzlich entfalten sie erst im Zusammenspiel ihre volle Wirkung.
Generell gilt außerdem: Je intensiver externe Experten (sowohl aus der Open-Data- als auch der Datenschutz-Community) eingebunden werden und Transparenz über Prozesse und Vorgänge geschaffen wird, desto größer wird auf allen Seiten die Akzeptanz für eine breitflächige Veröffentlichung von Daten der öffentlichen Hand sein – auch dann, wenn einmal etwas schief gehen sollte.

1. Vor der Veröffentlichung: Entscheidung, ob Daten überhaupt geöffnet werden dürfen bzw. sollen

Mögliche Risiken, die bei dieser Entscheidung auftreten können:

- Daten, die nicht veröffentlicht werden dürfen oder sollten, werden irrtümlich bzw. infolge unzureichender Prüfung als Open Data veröffentlicht.
- Das Abwägungsprinzip wird unzureichend angewandt und das Recht auf Privatsphäre nicht hinreichend berücksichtigt.
- Das Datenschutz-Argument wird missbraucht, um relevante Datensätze mit hohem gesellschaftlichen Mehrwert nicht zu öffnen.

Beispiele aus dem Ausland, die diese Risiken verdeutlichen:

- In Bhutan stellt man die Daten von Bewerbern auf öffentliche Stellen inkl. Kontaktdaten als offene Daten auf der Regierungsplattform bereit (Hintergrundgespräch mit NGO-Vertreter aus Bhutan).
- Die Stadt Washington, D.C. veröffentlichte Wählerdaten inkl. Name, Adresse und politische Präferenzen. http://fusion.net/story/314062/washington-dc-board-of-elections-publishes-addresses
- Für einen Hackathon stellten die Ausrichter Mobilfunkdaten (Call Detail Records) auf einer Online-Plattform zum Download zur Verfügung. https://responsibledata.io/reflection-stories/open-data-hackathon
- Die polnische Regierung veröffentlichte Daten über die Empfänger bestimmter Sozialleistungen mit Namen und Adressen (Hintergrundgespräch mit NGO-Vertreter aus Polen).

Prozessvorschlag

Datenbereitsteller werden über Materialien aus einer Art Werkzeugkasten über Datenschutzrisiken und Maßnahmen informiert. Für die Bewertung der Daten steht dem Mitarbeiter eine Checkliste als Entscheidungshilfe zur Verfügung. Diese bildet ein Vorgehensmodell für die Datenöffnung ab und liefert die Bewertungsgrundlage, ob Daten geöffnet werden sollen oder nicht. Die Daten werden so vom Datenbereitsteller (Sachbearbeiter) anhand eines Ampelsystems im Sinne einer Risikoprüfung bewertet. Das Bewertungsschema muss zwingend in regelmäßigen Abständen auf Aktualität und Richtigkeit geprüft werden. **Rote Datensätze** werden nicht veröffentlicht, **grüne** werden im Sinne der Open-Definition veröffentlicht. **Orange** Datensätze durchlaufen eine Art abgeschwächtes Privacy Impact Assessment. Bei der Klassifizierung in unbedenklich (grün), nicht zu veröffentlichen (rot) und zu prüfen (orange) ist das Vier-Augen-Prinzip zu befolgen, d. h. mindestens zwei Personen der jeweiligen Behörde müssen zum gleichen Ergebnis kommen. Ist dem nicht so, muss der Fall über eine dritte Instanz, etwa die geplante Open-Data-Beratungsstelle, eskaliert werden.

Neben dieser Beratung erarbeitet die zu schaffende Open-Data-Beratungsstelle die Materialien, die den Bearbeitern als Hilfestellung dienen sollen. Dabei kann auch direkt auf Expertise der Bundesdatenschutzbeauftragten zurückgegriffen werden.
Über Datensätze, die eine hohe soziale Relevanz haben oder die intensiv angefragt werden, entscheidet ein externes Beratungsgremium, das sich aus Vertretern der jeweiligen Behörde, der Open-Data-Community und Datenschutzexperten zusammensetzt.

		Instrument	Chance / Vorteil	Risiko / Nachteil	Beispiele
1.1	KF	**Bewertungshilfe** **Werkzeugkasten für Open-Data-Veröffentlichung** (etwa Vorgehensmodell, Merkblätter, Ansprechpartner)	• Wenn anschaulich aufbereitet, gute Hilfestellung für Verwaltungsmitarbeiter, um adäquate Datensätze zu identifizieren • Wenn offen zur Verfügung gestellt bzw. sogar kollaborativ erarbeitet, erzeugt dies Vertrauen seitens der Community	• Wenn unvollständig, werden weitergehende Herausforderungen für den Datenschutz nicht berücksichtigt • Ständige Revision dringend erforderlich	Siehe „Open Data Release Toolkit“ der Stadt San Francisco: https://drive.google.com/file/d/0B0jc1tmJAlTcR0RMV01PM2NyNDA/view Siehe „Handreichung Datenschutz“ des Rats für Sozial- und WirtschaftDaten: https://www.ratswd.de/dl/RatSWD_Output5_HandreichungDatenschutz.pdf
1.2	KF	**Bewertungshilfe** **Checklisten zur Bewertung des generellen Datenschutzrisikos, das von Datensätzen ausgeht** (idealerweise als Teil des Werkzeugkastens unter 1.1)	• Baut Unsicherheiten der Verwaltungsmitarbeiter ab • Gutes Material als Anregungen aus dem Ausland verfügbar	• Bewertungskriterien und Standards entwickeln und verändern sich mit der Zeit • Die Listen müssen daher (nicht oft, aber regelmäßig) auf Aktualität und Angemessenheit überprüft werden • Checklisten tragen evtl. dazu bei, dass Beurteiler automatisch nach Schema X vorgehen	Siehe „Open Data Release Form“ der Stadt San Francisco: https://docs.google.com/document/d/12uk04YOXqP10oqFy6EcJ-wRa0IrGx1B-BaCNUITP-EA/edit
1.3	MF	**Bewertungshilfe** **Ampelsystem zur Kategorisierung von Datensätzen nach potenziellem Datenschutzrisiko** **Grün** = Datensatz kann bedenkenlos als Rohdaten (nicht-anonymisiert) geöffnet werden **Rot** = Datensatz darf so auf keinen Fall geöffnet werden **Orange** = Datensätze müssen zunächst eine Prüfung durchlaufen und können ggf. unter Berücksichtigung bestimmter Schutzmaßnahmen geöffnet werden	• Deutliche Erleichterung für Datenbereitsteller • Gesteigerte Akzeptanz, wenn Bewertungskatalog für die Kategorisierung offengelegt oder gar kollaborativ mit der Zivilgesellschaft erarbeitet wird	• Risiken können (und werden) sich ändern • Muss daher ständig aktualisiert werden • Könnte evtl. dazu beitragen, Risiken zu verharmlosen	Siehe z. B. Vorschläge aus der Forschung von Zuiderveen Borgesius et al. (2015): https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2695005, oder den Ansatz des sechsstufigen „Datatag System“ von Sweeney et al. (2015): http://techscience.org/a/2015101601 Siehe „Open Data Release Toolkit“ der Stadt San Francisco: https://drive.google.com/file/d/0B0jc1tmJAlTcR0RMV01PM2NyNDA/view Siehe PSI-Bewertungsmodell der österreichischen Regierung: https://www.ref.gv.at/fileadmin/_migrated/content_uploads/psi-klassifikation_1-0-0_20150622.pdf

1.4	KF	**Bewertungshilfe** (gilt bezogen auf 1.1 – 1.3) **Erarbeitung maßgeschneiderter Lösungen für bestimmte Themenfelder und/oder Behörden**	• Adressiert die Herausforderung, dass Datenschutzrisiken in einzelnen Behörden unterschiedlich hoch sind, da einige Behörden über sensiblere Daten verfügen als andere (vgl. z. B. Gesundheitsdaten)	• Die Risiken einzelner Bereiche könnten vorab in Gänze nur schwer abzuschätzen sein; von daher Einteilung/Priorisierung vermutlich nur schwer möglich	
1.5	MF	**Bewertungshilfe** **Nutzung eines vereinfachten Privacy Impact Assessment für orange Daten** (idealerweise als Teil des Werkzeugkasten unter 1.1)	• Wenn anschaulich aufbereitet, sinnvolles – und in anderen Bereichen etabliertes – Verfahren, um schwierige Datensätze zu identifizieren und zu bewerten • Wenn offen zur Verfügung gestellt bzw. sogar kollaborativ erarbeitet, erzeugt dies Vertrauen seitens der Community	• Ggf. abschreckend, wenn nur in „Juristen-Deutsch“ oder als Bleiwüste verfügbar • Um entsprechende Instrumente erstellen zu können, müsste zunächst eine umfangreiche Bottom-up-Analyse bestehender Fälle (idealerweise auch aus dem Ausland) durchgeführt werden • Zeitliche Verzögerung der Datenveröffentlichung • Komplexität	Siehe als Grundlage das Material des britischen Datenschutzbeauftragten zu Privacy Impact Assessments: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf Siehe Bieker et al. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation, S.27: http://link.springer.com/chapter/10.1007/978-3-319-44760-5_2
1.6	KF	**Institutionalisierung** **Prüfung zu veröffentlichender Datensätze nach dem Vier-Augen-Prinzip (als Bestandteil von 1.1 - 1.4);** bei Uneinigkeit Klärung mit unabhängiger Stelle (z. B. Beratungsstelle des BMI); bei orangen Daten mindestens mit dem Datenschutzbeauftragten der Behörde	• Vermeidung von Irrtümern • (Möglichst) Kompetenzmischung		*(Eigentlich normales und bewährtes Verfahren der Verwaltung auch in anderen Bereichen.)*

1.7	KF/ MF	**Institutionalisierung** **Zentrale Beratungsstelle Open Data für alle Behörden, die bei Unsicherheiten in den zuständigen Behörden unterstützt** (z. B. bei Uneinigkeit bzgl. oranger Datensätze) (Aktuell im Rahmes des Open-Data-Gesetzes vorgesehen.)	• Klarer Ansprechpartner für Datenbereitsteller • Hilfreich, insb. wenn technische und Datenschutzexpertise in der Stelle gegeben ist	• Bindet (noch zu schaffende) Ressourcen	
1.8	LF	**Institutionalisierung** **Externes Beratungsgremium (vgl. Ethik-Kommissionen), das mit über Daten von großer gesellschaftlicher Bedeutung, aber tendenziell hohen Datenschutzrisiken entscheidet** (z. B. Daten zu Flüchtlingen, Gesundheit, Smart Cities)	• Erhöht Akzeptanz in der Gesellschaft • Stärkt Bindung mit der Community • Gut an Open-Government-Partnership-Aktivitäten anbindbar • Hilfreich, um sich wandelnden Zeitgeist abzubilden, etwa bezügl. Datensätze, deren Veröffentlichung auf einmal als besonders wichtig erachtet werden (wie etwa in den USA die Veröffentlichung von Polizeistatistiken, um Diskriminierung aufzudecken), oder aber der Klassifizierung von bislang unproblematischen Daten in risikoreiche Daten (wie etwa mit Datensätzen zu Flüchtlingsunterkünften geschehen)	• Akzeptanz bei Verwaltungsmitarbeitern ggf. nicht ausreichend gewährleistet • Legitimation kann von außen angezweifelt werden	Siehe als Inspiration die Open-Government-Diskussionsplattform des UK Open Government Network: http://www.opengovernment.org.uk/engage, sowie den zivilgesellschaftlichen Konsultationsprozess der britischen Regierung zu „Data Sharing“: http://www.datasharing.org.uk (allerdings nur einmalig), in Anlehnung an die Empfehlung 6 („Create sector transparency panel“) von O’Hara (2011): https://eprints.soton.ac.uk/272769/1/272769OHARA11.pdf

2. Bei der Veröffentlichung: Maßnahmen im Zuge der Veröffentlichung von Daten

Mögliche Risiken, die bei der Veröffentlichung entstehen können:

- Schlechte oder unzureichende Anonymisierung
- Möglichkeit der Reidentifizierung trotz Anonymisierung

Beispiele aus dem Ausland, die diese Risiken verdeutlichen:

- Nach der Veröffentlichung anonymisierter Taxi-Daten in New York konnten Hacker das Gehalt von Taxifahrern, die Bewegungsmuster von Prominenten sowie die Wohnorte einzelner Fahrgäste identifizieren. https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset
- Das ÖPNV-Unternehmen Transport for London publizierte Daten über die Nutzung öffentlicher Fahrräder, die deanonymisiert werden konnten und die Erstellung von Bewegungsmustern einzelner Radfahrer erlaubte. http://qz.com/199209/londons-bike-share-program-unwittingly-revealed-its-cyclists-movements-for-the-world-to-see
- Auf einem australischen Open-Data-Portal wurden – anonymisierte – Daten u. a. über Rezeptverschreibungen veröffentlicht. Die Universität Melbourne zeigte, dass eine Verknüpfung dieser Daten mit anderen Datensätzen Rückschlüsse auf einzelne Ärzte zuließ.
- Die britische Regierung stellte sensible Gesundheitsdaten ihrer Bürger auf der Plattform care.data bereit, ohne diese hinreichend zu informieren oder zu Beginn um ihre Einwilligung zu bitten. Der Datenzugang war zwar nur mit Registrierung möglich und die Daten pseudonymisiert, doch die Privatsphäre der Bürger war de facto nur marginal geschützt, zumal intransparent blieb, wer alles Zugriff auf die Daten erhalten sollte. Der Widerstand in der Bevölkerung war groß und führte zur Einstellung des Projekts. https://www.theguardian.com/technology/2016/jul/06/nhs-to-scrap-single-database-of-patients-medical-details

Prozessvorschlag

Im vorgeschlagenen Ampelsystem als orange eingestufte Datensätze können eventuell nach einer Anonymisierung veröffentlicht werden. Damit dies qualitativ hochwertig und zügig gelingt, müssen technische Instrumente eingesetzt werden, um eine hohe Anonymisierungsqualität zu erreichen. Darüber hinaus müssen entsprechende Fortbildungen für die Mitarbeiter angeboten werden.
Eingesetzte Anonymisierungsverfahren sind vorab von Experten zu evaluieren. Außerdem werden sie bei Veröffentlichung der Daten als Metadaten dokumentiert. Zu prüfen ist, inwiefern sich Privacy-by-design-Lösungen in Datenplattformen integrieren lassen. Generell sollte die Entwicklung und Implementierung nutzerfreundlicher technischer Maßnahmen für eine qualitativ hochwertige Anonymisierung gefördert werden.

		Instrument	Chance / Vorteil	Risiko / Nachteil	Beispiele
2.1	KF	**Kapazitätsaufbau** **Leitfäden für die Aggregierung und die Anonymisierung von Daten**	• Orientierung und Arbeitserleichterung, wenn anschaulich aufbereitet • Kompetenzenaufbau für technischen Datenschutz	• Der Nutzen aus Daten sinkt normalerweise umgekehrt proportional zum Aggregierungsgrad • Kann Fehler nicht ausschließen • Gute Anonymisierung ist schwierig, daher fraglich, ob Leitfäden reichen	Siehe hier den „Code of Practice“ für Anonymisierung des britischen Datenschutzbeauftragten: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
2.2	KF	**Kapazitätsaufbau** **Trainings für Datenbereitsteller im Hinblick auf Anonymisierung** (über Kurse, Online-Tools, Blended-Learning-Angebote)	• Steigert erforderliche Kompetenzen für technischen Datenschutz	• Bindet Ressourcen und braucht Zeit	Siehe als erste Anregung etwa die Materialien des UK Anonymisation Networks, z. B. das „Anonymisation Decision-Making Framework“: http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf, oder die „Case Studies“: http://ukanon.net/ukan-resources/case-studies
2.3	MF	**Technischer Datenschutz** **Nutzung technischer Anwendungen, die hochwertige Anonymisierung erlauben** (Stichwort Privacy Enhancing Technology)	• Höheres Datenschutzniveau • Empowerment von Datenbereitstellern	• Verlass auf die Technik lässt Fehler möglicherweise schneller übersehen, der Kapazitätsaufbau innerhalb der Stellen muss deswegen vorab stattfinden • Oft sind Anwendungen nicht besonders nutzerfreundlich	Siehe die Softwarelösungen von ARX – Data Anonymization Tool: http://arx.deidentifier.org, oder von Aircloak: https://www.aircloak.com
2.4	KF	**Institutionalisierung** **Verzeichnung der Art der Anonymisierung als Metadaten**	• Erleichtert Fehlererkennung und Fehlervermeidung • Entsprechende technische Verfahren (2.3) könnten dies automatisieren • Erleichtert die Risikoprüfung nach 3.5 bzw. 3.6	• Erhöht ggf. das Risiko gezielter Deanonymisierung	

2.5	MF	**Institutionalisierung** **Externe Prüfung von Anonymisierungsverfahren** Einbindung von Experten über Konsultationsprozess, um Anonymisierungsqualität zu prüfen; erneute Prüfung in regelmäßigen Abständen	• Stellt hohe und zeitgemäße Standards der Anonymisierung sicher • Dynamische Anpassung an technische Entwicklungen • Stärkt Akzeptanz und Vertrauen	• Zusätzlicher Schritt, der Ressourcen bindet und Zeit kostet • Sorgt evtl. für Verzögerung von weiterer Datenöffnung	Siehe den Vorschlag australischer Wissenschaftler gewählte Anonymisierungverfahren der Behörden von Experten vorab prüfen zu lassen: https://pursuit.unimelb.edu.au/articles/crime-and-privacy-in-open-data
2.6	LF	**Technischer Datenschutz** **SafeAnswer-Anwendungen für sensible Daten,** technische Anwendungen, die Anfragen an Datensätze, aber kein Zugang zu Rohdaten zulassen	• Deutlich gesteigerter Datenschutz • Ermöglicht auch die Nutzung von sensiblen Daten • Förderung und Forschung in derartige Systeme könnte langfristig Datenschutzproblematik lösen	• Noch im Forschungsstadium • Entspricht nicht der Open-Definition	Siehe die Anwendung der SafeAnswer-Technologie bei OpenPDS: http://openpds.media.mit.edu Siehe den Ansatz der Differential Privacy: https://blog.cryptographyengineering.com/2016/06/15/what-is-differential-privacy
2.7	LF	**Technischer Datenschutz** **Privacy by design für Fachanwendungen und Datenplattformen**, z. B. automatisierte Anonymisierung	• Höheres Datenschutzniveau • Empowerment von Datenbereitstellern	• Verlass auf die Technik lässt Fehler möglicherweise schneller übersehen • Anonymisierung begrenzt bereits Nutzungspotenziale, sinnvolle und wirksame Anonymisierung hängt stets stark von späterer Nutzung ab	Siehe z. B. den Ansatz einer Datennutzungskontrolle, wie er im Projekt IND²UCE des Fraunhofer IESE verfolgt wird: https://www.iese.fraunhofer.de/de/competencies/security/ind2uce-framework.html; vgl. dazu auch 3.2 (Datenzugangskontrolle)

3. Nach der Veröffentlichung: Steuerung der Nutzung von geöffneten Daten

Risiken, die durch einmal geöffnete Daten entstehen können:

- Durch die beschriebenen Grenzen der Anonymisierung könnten Daten mit anderen öffentlich zugänglichen Daten in Verbindung gebracht werden, wodurch ggf. eine Deanonymisierung möglich wird.
- Offene Daten werden Teil des größeren „Datenkosmos“ und können so ohne das Wissen der Betroffenen von Datenhändlern für die Profilbildung genutzt werden. Damit könnten sie, ebenso wie andere Daten, etwa von Versicherungs- oder Kreditanbietern für die Tarifbildung verwendet werden.

Beispiele aus dem Ausland, die diese Risiken verdeutlichen:

- In Minneapolis wurden die Daten von Kfz-Kennzeichenlesern nach der Veröffentlichung von Datenhändlern weiterverarbeitet. Dies führte zu massiver öffentlicher Empörung. http://openscholar.mit.edu/sites/default/files/dept/files/modernopendataprivacy.pdf
- In Seattle wurden offene Regierungsdaten von Datenhändlern genutzt, um in Kombination mit anderen Daten Profile von Bürgern zu erstellen und diese beispielsweise an Werbetreibende weiterzuverkaufen. http://btlj.org/data/articles2015/vol30/30_3/1899-1966%20Whittington.pdf

Prozessvorschlag

Über die Grenzen von Anonymisierungsverfahren und empfehlenswerte Vorgehensweisen wird auf Open-Data-Plattformen proaktiv informiert. Sensible Datensätze werden lediglich mit einem restriktiven Zugang zugänglich gemacht. Welche Datensätze als sensibel einzustufen sind, wird in Absprache mit einem externen Beratungsgremium beschlossen. Um gegen Deanonymisierung vorzugehen, wird die Verbreitung und Nutzung deanonymisierter Datensätze in Anlehnung an die statistikrechtliche Praxis sanktioniert. In jeder veröffentlichenden Stelle werden Prozesse aufgesetzt, wie mit potenziell gefährdeten Datensätzen umgegangen werden kann (Nicht-Veröffentlichung, restriktiver Zugang, verbesserte Anonymisierung etc.). Fälle werden gesammelt und ausgewertet, um Fehler zukünftig zu vermeiden und ein Frühwarnsystem zu entwickeln. In regelmäßigen Abständen werden die bereitgestellten Datensätze auf Risiken der Deanonymisierung geprüft, was durch interne Bearbeiter oder externe Experten erfolgen kann.

		Instrument	Chance / Vorteil	Risiko / Nachteil	Beispiele
3.1	KF	**Kapazitätsaufbau** **Aufklärung über Anonymisierungsverfahren und deren Grenzen auf Open-Data-Plattformen und über andere Medien,** ggf. inkl. Zertifizierung von Plattformen bzgl. Privacy-Berücksichtigung	• Proaktive Hinweise auf Herausforderungen können vertrauensbildend wirken • Kann auch als Referenz genutzt werden für den Fall, dass etwas schief geht	• Wirkt nur aufklärend, aber minimiert nicht das unmittelbare Risiko	Siehe Erläuterung der Anonymisierungsverfahren auf Webseite von UK Police Data: https://data.police.uk/about/#anonymisation
3.2	MF	**Regulierungsansatz** **Restriktiver Zugang für registrierte oder sogar zertifizierte Nutzer oder auf spezielle Anfrage,** z. B. durch Forscher	• Höherer Sicherheitsstandard durch Überprüfbarkeit von Datennutzern • Ermöglicht den Zugang zu relevanten, jedoch risikoreicheren Datensätzen	• Entspricht nicht der Open-Definition • Bürokratischer Mehraufwand	Siehe den Ansatz aus San Francisco, nach dessen Bewertungsschema einige Datensätze nur restriktiv zur Verfügung gestellt werden („Open Data Release Toolkit“, S. 19): https://drive.google.com/file/d/0B0jc1tmJAlTcR0RMV01PM2NyNDA/view Siehe z. B. den Ansatz einer Datennutzungskontrolle, wie er im Projekt IND²UCE des Fraunhofer IESE verfolgt wird, vgl. dazu auch Punkt 2.8
3.3	LF	**Regulierungsansatz** **Sanktionierung der Verbreitung und Nutzung deanonymisierter Daten**	• Kann bei hohen Strafen Weitergabe von deanonymisierten Daten einschränken	• Internationaler Datenfluss macht nationale Regulierung nur bedingt wirksam • Entspricht nicht der Open-Definition • Abhängig von wirksamer Rechtsdurchsetzung	Siehe die Empfehlung australischer Wissenschaftler (gegen die Entscheidung der australischen Regierung): https://pursuit.unimelb.edu.au/articles/crime-and-privacy-in-open-data Datenschutzgesetze schränken bereits die weitere Verwendung öffentlicher Daten insofern ein, als berechtigte Interessen evtl. betroffener Personen nicht unverhältnismäßig beeinträchtigt werden dürfen. Siehe auch Ausführungen im Statistikgesetz zur Untersagung vorsätzlicher Reidentifizierung, siehe § 21 des Bundesstatistikgesetzes zum Verbot der Reidentifizierung.
3.4	MF	**Kapazitätsaufbau** **Etablierung von Prozessen, um mit Deanonymisierung umzugehen,** z. B. Anleitung zur schnellen Entfernung von Daten (inkl. Reporting)	• Effiziente Prozesse essenziell, um größere Risiken zu verhindern • Reporting unterstützt Akzeptanz • Gutes Fehlermanagement hilft, ähnliche Fehler künftig zu vermeiden	• Wirkt lediglich als Schadensbegrenzung und nicht gegen die tatsächlichen Risiken	Siehe hier die Empfehlung aus der Studie des BMI „Open Government Data Deutschland“, „organisatorische Prozesse für die Reanonymisierung zu etablieren“: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/ModerneVerwaltung/opengovernment.pdf?__blob=publicationFile

3.5	MF	**Institutionalisierung** **Jährliche generelle Risikoprüfung der Open-Data-Aktivitäten auf Datenschutzrisiken**	• Dynamische Anpassbarkeit • Notwendige Zusammenarbeit mit Wissenschaft fördert Community-Building	• Erfordert Ressourcen • Begrenzt lediglich den Schaden	Siehe die „Open Data Policy“ von Seattle: http://www.seattle.gov/Documents/Departments/SeattleGovPortals/CityServices/OpenDataPolicyV1.pdf
3.6	MF	**Institutionalisierung** **Stetig forcierte Prüfung auf mögliche Reidentifizierungsrisiken von außen** (ggf. Bescheinigung der Prüfung auf Open-Data-Plattformen ähnlich einer Zertifizierung, siehe 3.1)	• Gut, um mit der Community in Kontakt zu kommen und an Privacy-Standards zu arbeiten • Dynamische Anpassung an technische Entwicklungen möglich	• Erfordert Ressourcen • Begrenzt lediglich den Schaden • Setzt Vertrauen in die und seitens der Community voraus	In Anlehnung an etablierte Verfahren aus der IT-Sicherheit: Auf Basis definierter Codes of Ethics werden sog. „Bug-Bounty-Programme“ (Angriffe durch externe Hacker zur Identifizierung von Systemschwachstellen) durchgeführt: https://en.wikipedia.org/wiki/Bug_bounty_program Siehe etwa das Angebot von Penetrationstests des Chaos Computer Clubs Oder über Wissenschaft: In Seattle hat ein Forschungsteam Daten auf Reidentifizierbarkeit geprüft
3.7	LF	**Institutionalisierung** **Aufbau eines Fehlerkatalogs** Fälle von Privacy-Verletzung sind meldepflichtig, werden (international) gesammelt und analysiert, um dann ein Frühwarnsystem daraus zu entwickeln	• Wirksames Instrument an sich und um Datenschutzexpertise in den Behörden aufzubauen • Hilft in Verknüpfung mit 2.4 Fehler besser zu verstehen und zukünftig zu vermeiden	• Dauert und muss kontinuierlich gepflegt werden • Hat keinen unmittelbaren Effekt	Siehe Vorgabe der EU-DSGVO, die zur Meldung von Data-Breaches verpflichtet, siehe „Notification of a personal data breach to the supervisory authority“ Art. 33, EU-DSGVO.
3.8	MF	**Regulierungsansatz** **Allgemeine Beschränkung der Datennutzung in Nutzungsbedingungen / Lizenzen**	• Setzt beim allgemeinen aktuellen Datendiskurs an • Verringert z. B. das Risiko, dass Daten diskriminierend genutzt werden	• Internationaler Datenfluss macht nationale Regulierung nur bedingt wirksam • Entspricht nicht der Open-Definition	Siehe hier das Archivrecht, nach dem die Nutzung von personenbezogenen Informationsbeständen nur zur Forschung zugelassen wird, sofern diese nicht veröffentlicht werden

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über das Projekt

Offene Verwaltungsdaten fördern die Entstehung neuer Geschäftsideen sowie neue Formen des zivilgesellschaftlichen und bürgerlichen Engagements. Die In-Wert-Setzung von Verwaltungsdaten stattet Behörden mit mehr Wissen und Kompetenzen aus und macht sie für's Digitalzeitalter fit. Das Projekt “Open Data & Privacy” treibt das Thema auf der politischen Agenda Deutschlands voran und bezieht den Datenschutz von Anfang an als Kernbestandteil mit ein. Im Austausch mit Stakeholdern aus Politik, Verwaltung, Zivilgesellschaft, Wirtschaft und Forschung entwickelt das Projekt konkrete Empfehlungen für einen Open-Data-Ansatz, der national tragfähig ist und die internationale Entwicklung auf diesem Feld voran bringt.

So erreichen Sie die Autoren:

Julia Manske
jmanske@stiftung-nv.de
Twitter: @juka_ma

Tobias Knobloch
tknobloch@stiftung-nv.de
Twitter: @tobiasknobloch

Impressum

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de
Twitter: @SNV_berlin

Design:
Make Studio
www.make-studio.net

Layout:
Franziska Wiese

Kostenloser Download:
www.stiftung-nv.de