Innovative Datenpolitik: Potenziale und Herausforderungen

Stellungnahme zur Anhörung des Ausschusses für Digitales am 26. Juni 2024

Elisa Lindinger, Co-Geschäftsführerin SUPERRR Lab

Inhalt

Über SUPERRR Lab 2
Unsere Empfehlungen in Kürze: 2
01. Datenschutz als Grundlage für eine chancengerechte Gesellschaft 3
Die besondere Rolle des Datenschutzes im Kontext der Digitalisierung 3
Gesamtgesellschaftlicher Datenschutz statt individuelle Verantwortlichkeit 4
02. Datenschutz als Gesellschaftsschutz im Kontext von Innovation 4
Zur These: Datenschutz als Innovationsbremse 5
Exkurs: Die Folgen unzureichenden Datenschutzes 5
Innovation ist mehr als ein Wirtschaftsmodell 6
03. Innovative Datenpolitik mit öffentlichen Daten: Status des Transparenzgesetzes 7
04. Datenpolitik im internationalen Kontext 8

Über SUPERRR Lab

SUPERRR Lab ist ein Labor für gerechte digitale Zukünfte. Als gemeinnützige Organisation arbeiten wir an Themen an der Schnittstelle von Technologie und Gesellschaft. Wir stellen bestehende Paradigmen der Digitalisierung in Frage, indem wir neue Perspektiven in die Diskussion rund um Technologie einbringen. Digitalpolitik ist für uns Gesellschaftspolitik. In unserer Forschungs- und Advocacy-Arbeit betrachten wir neue Technologien, Technologieregulierung und andere digitalpolitische Vorhaben mit Fokus auf ihre gesellschaftlichen Auswirkungen. Wir hinterfragen Machtverhältnisse in der Digitalisierung und setzen uns für eine Stärkung der Grundrechte ein. Unsere Arbeit wird von feministischen Werten wie Gerechtigkeit, Zugang, Mitgestaltung und Nachhaltigkeit angetrieben.

Unsere Empfehlungen in Kürze:

1. Datenschutz ist in einer diversen Gesellschaft ein wirksames Mittel gegen datenbasierte Diskriminierung und Profiling und darf deshalb nicht gegen wirtschaftliche Interessen abgewogen werden.

2. Datenschutz muss für alle erreichbar sein. Deshalb sind Ansätze wie die Förderung von Data Literacy und Datensouveränität (im Sinne einer freiwilligen Verfügbarmachung) hilfreiche ergänzende Maßnahmen, aber kein Ersatz für einen starken Datenschutz, der keiner individuellen Umsetzung bedarf.

3. Eine innovative Datenpolitik muss die technischen Voraussetzungen und Best Practices für verantwortungsvolle Datenhaltung fördern.

4. Für die Erforschung der gesellschaftlichen Auswirkungen von massiven Datenschutzverletzungen sind eine bessere Dokumentation und mehr Ressourcen notwendig.

5. Ein Transparenzgesetz, das den Zugang zu und die Nutzung von öffentlichen Daten und Informationen bundesweit regelt, ist so schnell wie möglich auf den Weg zu bringen.

1. Datenschutz als Grundlage für eine chancengerechte Gesellschaft

Der Schutz personenbezogener Daten (kurz: Datenschutz) ist ein Grundrecht.[1] In einer pluralistischen, diversen Gesellschaft ist funktionierender Datenschutz eine notwendige Voraussetzung für die Teilhabe aller am öffentlichen, demokratischen Leben. Er erschwert mögliche datenbasierte Diskriminierung, beispielsweise durch Anwendung maschineller Lernverfahren. Im Gegensatz zum Antidiskriminierungsrecht setzt er schon bei der Erhebung von Daten an und hat so das Potenzial, Diskriminierung vorzugreifen und sie aktiv zu verhindern.[2] Das macht ihn zu einem essenziellen Regelwerk für eine innovative, aber gerechte Digitalisierung.

Die besondere Rolle des Datenschutzes im Kontext der Digitalisierung

Im Kontext der digitalen Transformation, in der fast kontinuierlich personenbezogene Daten bei der Nutzung digitaler Dienste erhoben und gespeichert werden, kommt dem Datenschutz eine besonders große Bedeutung zu. Vor diesem Hintergrund entstand die Datenschutz-Grundverordnung (DS-GVO), die die vorher gültige Datenschutzrichtlinie präzisiert und ergänzt, um Europa „fit fürs Digitale Zeitalter“ zu machen.[3]

Der Schutz personenbezogener Daten darf nicht nur dann gewährleistet sein, wenn Individuen über ausreichend Wissen, Zeit und Ressourcen verfügen, Datenschutzverstöße zu erkennen und ihrem Recht Geltung zu verleihen. In einer Gesellschaft, in der Menschen unterschiedlichen Zugang zu Bildung haben unterschiedlich viel Zeit mit bezahlter und unbezahlter Arbeit verbringen, kann die Auslagerung der Rechtsdurchsetzung nicht die Aufgabe der einzelnen Person sein. Denn das führt dazu, dass sich viele nicht ausreichend vor Profiling, ungewolltem Handel mit ihren Daten und daraus resultierender datenbasierter Diskriminierung schützen können.

Frage 3

Gesamtgesellschaftlicher Datenschutz statt individuelle Verantwortlichkeit

Wir unterstützen Forderungen nach mehr Medienkompetenz und Digital Literacy. Im Kontext einer starken Datenschutzgesetzgebung und wirkungsvoller Rechtsdurchsetzung sind sie hilfreich, um Menschen für die Relevanz ihrer per-

1 gem. Art. 8 GRCh und DS-GVO.
2 https://stiftungdatenschutz.org/praxisthemen/kuenstliche-intelligenz-und-gleichstellung
3 https://www.europarl.europa.eu/news/de/press-room/20160407IPR21776/parlament-verabschiedet-eu-datenschutzreform-eu-fit-furs-digitale-zeitalter?quizBaseUrl=https%3A%2F%2Fquizweb.eurWWoparl.europa.eu

sonenbezogenen Daten zu sensibilisieren. Sie können konkrete Ansätze vermitteln, wie und wo sich personenbezogene Daten bestmöglich schützen lassen.

Wir sind jedoch der Ansicht, dass Digital Literacy allein nicht ausreicht, da sie die Verpflichtung für den Schutz personenbezogener Daten vor allem auf das Individuum verschiebt, statt Unternehmen und Diensteanbieter in die Pflicht zu nehmen. Dasselbe trifft auf das Konzept von Datensouveränität zu: Der unscharfe Begriff[4] bezeichnet in der Tendenz eine „individuelle Kontrollierbarkeit von Daten und deren Verarbeitung".[5] Unserer Ansicht nach darf sich diese Kontrolle aber nicht auf den Schutz von Daten beziehen, sondern nur auf eine freiwillige Verfügbarmachung personenbezogener Daten, beispielsweise für gemeinwohlorientierte Forschung (Datenspende). Datenschutz muss stets der Default sein, um diejenigen vor ungewollter Datenweitergabe zu schützen, die sich nicht mit den Details technischer Systeme auseinandersetzen können.

Frage 3

In einer Gesellschaft aus Menschen mit unterschiedlichem Bildungsstand, finanziellem Status und zeitlichen Ressourcen führt eine solche Verschiebung automatisch zu einer Zwei-Klassen-Gesellschaft im Digitalen. Das widerspricht der Idee der Chancengleichheit.

2. Datenschutz als Gesellschaftsschutz im Kontext von Innovation

In der Göttinger Erklärung hat die Datenschutzkonferenz 2017 das vermeintliche Spannungsfeld von Datenschutz und Innovation bewertet: „Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. (...) Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen."[6]

Zur These: Datenschutz als Innovationsbremse

Datenschutz wird häufig als Hemmnis für Innovation angeführt und gilt als Ursache für wirtschaftliche Nachteile von Unternehmen. Grundrechte sind aber nicht gegen wirtschaftliche Interessen abwägbar. Selbst Umfragen unter Unternehmen zu dem Ergebnis, dass als größte Herausforderung bei der Implementierung der DS-GVO mit 78% nicht der Datenschutz an sich, sondern die Rechtsunsicherheit angeführt wird. Auch die DS-GVO selbst wird nicht in Frage gestellt, sondern Bedarf nach mehr „praktischen Lösungskonzepten" angemeldet.[7]

Frage 3

Solche Lösungskonzepte fehlten auch deshalb, weil die vor der DS-GVO gülti-

4 https://www.bidt.digital/glossar/datensouveraenitaet/
5 Hummel, P., Braun, M., Augsberg, S., Ulmenstein, U.v., Dabrock, P. (2021). Datensouveränität als informationelle Freiheitsgestaltung. In: Datensouveränität. essentials. Springer VS, Wiesbaden. https://doi.org/10.1007/978-3-658-33755-1_1
6 https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20173003_Entschliessung_Wert_Datenschutzes.pdf?__blob=publicationFile&v=6
7 https://www.bitkom.org/sites/main/files/2023-01/Studie-Datenschutz-als-Herausforderung-fur-die-Digitalisierung-final.pdf

gen Regelungen beispielsweise in Deutschland nicht umfassend durchgesetzt wurden und so kein Anreiz für innovative, gesetzeskonforme Anwendungen bestand.[8] Mit der DS-GVO wurde nun die Durchsetzung verbessert, wie die Zahl an verhängten Bußgeldern zeigt.[9] Diese Strafen und damit einhergehende Auflagen für Unternehmen haben dazu beigetragen, dass sich die Sicherheitsstandards in Unternehmen erhöht haben.[10] Gleichzeitig bewerten zivilgesellschaftliche Organisationen die DS-GVO als „absoluten Mindeststandard".[11]

Exkurs: Die Folgen unzureichenden Datenschutzes

Datenschutzverletzungen haben gesellschaftliche und damit direkt oder indirekt auch wirtschaftliche Auswirkungen, zeigen nationale und internationale Beispiele. Die finnische Firma Vastaamo, ein Service-Anbieter für Psychotherapeut*innen, verarbeitete Daten von Patient*innen und Therapiesitzungen ohne ausreichende Sicherheitsstandards und speicherte sie ohne Pseudonymisierung.[12] Aufgrund großer IT-Sicherheitmängel konnten die Daten von einem Angreifer abgerufen werden und wurden dazu verwendet, rund 30.000 Patient*innen mit den Inhalten aus ihren Therapiesitzungen zu erpressen, darunter auch Politiker*innen. Die Erpressungsversuche führten bei vielen nicht zuletzt therapiebedürftigen Patient*innen zu Angstzuständen, Stress und Trauma.[13] Neben dem individuellen Schaden entstand auch ein gesellschaftlicher Schaden (Vertrauensverlust in digitale Dienste über die konkrete Anwendung von Vastaamo hinaus) sowie ein wirtschaftlicher Schaden, auch wenn dieser aufgrund mangelnder Forschung kaum quantifizierbar ist.[14] Eine gezielte wissenschaftliche Begleitung im Nachgang von Datenschutzverletzungen kann hier Abhilfe schaffen.

Frage 6
Frage 9
Frage 13

Wir erkennen an, dass die umfassende Absicherung eigener digitaler Infrastrukturen und damit auch von darin gespeicherten oder vermittelten Daten besonders für kleine und mittlere Unternehmen eine Herausforderung ist. Das ist jedoch keine Entschuldigung für Nachlässigkeit beim Datenschutz oder der Datensicherheit. Große Infrastrukturprojekte wie GAIA-X müssen stattdessen Datenschutz von Anfang an mitdenken und die Voraussetzungen dafür schaffen, dass Unternehmen, die die digitalen Infrastrukturen nutzen, Datenschutzgrundsätze wie Transparenz, Datenübertragbarkeit und vor allem Privacy by Default möglichst einfach umsetzen können.

Innovation ist mehr als ein Wirtschaftsmodell

Frage 16

Innovation ist nicht gleich Innovation: Neben wirtschaftlicher Innovation durch neue Geschäftsmodelle kann Innovation auch rein technisch sein, z. B. in Form von neuen Verfahren oder Implementierungen. Eine innovative Datenpolitik muss solche Verfahren fördern, die Datenschutzvorgaben technisch umsetzen.

8 https://publica-rest.fraunhofer.de/server/api/core/bitstreams/36ffbb27-a0be-45d0-b0d9-ca189127205b/content
9 https://www.enforcementtracker.com/
10 https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement
11 https://edri.org/our-work/eu-data-protection-package-lacking-ambition-but-saving-the-basics/
12 Zur Entscheidung des EDPB: https://www.edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_de
13 https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/
14 Zum noch laufenden Entschädungsprozess des finnischen Finanzministeriums: https://www.valtiokonttori.fi/en/services/services-related-to-compensation-and-accidents/vastaamo/#_what-will-be-compensated

Nur dann können darauf auch solide und verantwortliche Geschäftsmodelle aufgebaut werden. Das zeigt das Beispiel der Anwendungen zur Kontaktnachverfolgung, die während der COVID19-Pandemie entwickelt wurden. Die Corona Warn App (CWA) setzte auf einige technisch solide Verfahren, auf Dezentralität und Pseudonymisierung und war damit sowohl in ihrem Entstehungsprozess als auch im Ergebnis ein Novum.

Frage 16

Zivilgesellschaftliche Organisationen haben wiederholt darauf hingewiesen, dass Kernkonzepte des Datenschutzes wie Datenminimierung bzw. Datensparsamkeit durch die technische Ausgestaltung der Anwendung essenziell für gemeinwohlorientierte Anwendungen sind.[15] Dass trotzdem, auch von der Politik, Anwendungen mit größerem Datenfußabdruck[16] favorisiert und sogar beauftragt wurden[17], ist vor dem Hintergrund bestehender, gut funktionierender und technisch ggf. innovativerer Alternativen schwer nachvollziehbar.

Dass trotz wiederholter Sicherheitslücken von CWA-Alternativen wie der Luca App kein größerer Schaden entstand, ist dem Engagement von Sicherheitsforscher*innen zu verdanken, die Sicherheitslücken aufdeckten und per responsible disclosure bekannt machten.[18]

3. Innovative Datenpolitik mit öffentlichen Daten: Status des Transparenzgesetzes

Eine innovative Datenpolitik basiert bei weitem nicht nur auf personenbezogenen Daten. Eine wichtige Grundlage für datengetriebene Dienste sind Informationen aus der öffentlichen Verwaltung. Sie sind auch eine Voraussetzung für informierte gesellschaftliche Debatten, für soziale Innovation und politische Teilhabe und Mitgestaltung, vor allem auf lokaler und kommunaler Ebene.[19]

Frage 4
Frage 17

Die Grundlage für einen besseren Zugang zu öffentlichen Daten soll ein Bundestransparenzgesetz schaffen, das die bestehenden Transparenzgesetze bzw. Informationsfreiheitsgesetze der Länder weiterentwickelt.[20] Der bereits für Dezember 2023 angekündigte Entwurf des Transparenzgesetzes muss jetzt schnellstmöglich auf den Weg gebracht werden. Hier sehen wir eine direkte und umsetzbare Möglichkeit, innovative Datenpolitik Wirklichkeit werden zu lassen.

Für eine sinnvolle Datennutzung ist es nur selten notwendig, Datenbestände zu zentralisieren. Maschinenlesbarkeit, Harmonisierung und Verknüpfung im Sinne von Linked Open Data ist dafür ausreichend. Von einer Zentralisierung raten wir ab. Das gilt insbesondere für Datenbestände mit personenbezogenen Daten.

15 Civil Liberties Union for Europe, 2021: COVID-19 Contact Tracing Apps in the EU: Lessons from Germany, S. 6–8 https://dq4n3btxmr8c9.cloudfront.net/files/XKDH18/COVID_19_Contact_Tracing_Apps_in_the_EU_Lessons_from_Germany.pdf
16 https://digikoletter.github.io/
17 Civil Liberties Union for Europe, 2021: COVID-19 Contact Tracing Apps in the EU: Lessons from Germany, S. 19–21 https://dq4n3btxmr8c9.cloudfront.net/files/XKDH18/COVID_19_Contact_Tracing_Apps_in_the_EU_Lessons_from_Germany.pdf
18 https://netzpolitik.org/2021/it-sicherheit-schon-wieder-desastroese-sicherheitsluecke-in-luca-app/
19 https://netzpolitik.org/2024/oeffentliches-geld-oeffentliches-gut-die-demokratie-vorwaertsverteidigen-durch-ein-transparenzgesetz/
20 Gemäß Koalitionsvertrag: https://www.bundesregierung.de/breg-de/aktuelles/koalitionsvertrag-2021-1990800

4. Datenpolitik im internationalen Kontext

Frage 1
Frage 4
Frage 7

Im Internetzeitalter muss Datenschutz über Landesgrenzen hinweg betrachtet und gestaltet werden. Neben Rechtsakten wie der DS-GVO, der EU-Datenverordnung und des Daten-Governance-Rechtsakts auf EU-Ebene findet das Thema Datenaustausch (und damit das Thema Datenschutz) auch zunehmend in globalen Policy-Arenen statt, beispielsweise im Kontext des Global Digital Compacts. Mit der Internationalen Datenstrategie hat die Bundesregierung als Ziel für ihr internationales Engagement vorgegeben, internationale Datenflüsse „unter Einhaltung der europäischen Datenschutzstandards und der EU-Grundrechte“ mitgestalten zu wollen. Die Bundesregierung sollte sich deshalb auf internationaler Ebene, beispielsweise beim Summit for the Future und den Verhandlungen zum Global Digital Compact, dafür einsetzen und kontinuierlich zivilgesellschaftliche Expertise einholen. Darüber hinaus ist eine sichtbare Einbindung von Wissenschaft und Zivilgesellschaft bei den anstehenden Verhandlungen bei der UN, z. B. in Form einer Delegation mit Teilnehmenden dieser Stakeholdergruppen, ein wichtiges Zeichen für einen kompetenten Einsatz für den globalen Datenschutz und eine grundrechtsstärkende Datenpolitik.