Digital Autonomy Hub
Technik souverän nutzen

ARBEITSPAPIER
April 2021

(In-)transparente Datenschutzerklärungen und digitale Mündigkeit

Digital Autonomy Hub

Inhalt

EDITORIAL	3
RECHT AUF DATENSCHUTZ	4
PRIVATSPHÄRENSCHUTZ BEI DER NUTZUNG DIGITALER TECHNOLOGIEN UND SERVICES: DER GRUNDTON MACHT DIE MUSIK	6
IT'S THE DEVELOPERS!	8
WIESO TRANSPARENZ NICHT AUSREICHT	10

EDITORIAL

Elisabeth Schauermann
Projektleitung Digital Autonomy Hub, Gesellschaft für Informatik e.V.

Datenschutzerklärungen begegnen uns überall im Alltag und in der Nutzung von digitalen Technologien werden wir immer wieder nach unserer Einwilligung für Datenverarbeitung gefragt. Für die meisten Menschen ist die Auseinandersetzung mit Datenschutzbestimmungen im Digitalen bisher jedoch wenig greifbar.

Mit dem Kompetenzzentrum *Digital Autonomy Hub – Technik souverän nutzen* haben wir das Ziel, allen Menschen einen reflektierten und selbstbestimmten Umgang mit ihren Daten zu ermöglichen. Vor diesem Hintergrund diskutierten wir im Februar im Rahmen eines WebTalks mit fünf Expert·innen Herausforderungen für Selbstdatenschutz und Lösungsansätze, um die Mündigkeit von Nutzer·innen zu erhöhen. Die Diskussionsrunde wurde aufgezeichnet und steht allen Interessierten zur Verfügung.[1]

Dieses Arbeitspapier ist eine Zusammenfassung der unterschiedlichen Perspektiven der Expert·innen, die an der Diskussionsrunde beteiligt waren. So betont die Vorsitzende der Stiftung Datenschutz **Prof. Dr. Anne Riechert** in ihrem Beitrag, dass das Recht auf Datenschutz in der Praxis umsetzbar ist und bereits Ansätze zu Verbesserungen der Kontrollrechte und des Einwilligungsmanagements existieren. **Susen Döbelt** und **Frank Kienzle** aus dem Forschungsprojekt PANDERAM sprechen sich dafür aus, Selbstdatenschutz für Nutzer·innen möglichst aufwandsarm zu ermöglichen, wobei das Bedürfnis nach Wahrung der Privatsphäre einen individuell unterschiedlich ausgeprägten Wert darstellt. **Dr. Frank Pallas,** Senior Researcher im Fachgebiet Information Systems Engineering der TU Berlin, sieht die Technisierung von Datenschutzerklärungen und Weiterentwicklung von Privacy Enhancing Technologies als wichtigen Baustein an. Die Landesbeauftragte für Datenschutz Schleswig-Holstein **Marit Hansen** plädiert dafür, nicht nur Transparenz als Grundlage für Datenschutz anzusehen, sondern auch das Risikobewusstsein der Menschen, Fairness und Rechtskonformität in den Blick zunehmen.

Das Team des Digital Autonomy Hubs
wünscht Ihnen viel Freude und
spannende Einsichten beim Lesen.

1 https://www.youtube.com/watch?v=1Ktl3ZJPOhI

RECHT AUF DATENSCHUTZ

Von Prof. Dr. Anne Riechert,
Stiftung Datenschutz

Das Recht auf Datenschutz ist in der Praxis umsetzbar. Es existieren bereits Ansätze zu Verbesserungen der Kontrollrechte und des Einwilligungsmanagements.

Kontrollrechte

Jede Person hat ein Recht auf Schutz der sie betreffenden personenbezogenen Daten – dies klingt selbstverständlich und ist auf europäischer Ebene in der Charta der Grundrechte der Europäischen Union verankert. Regelungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, z.B. Kontrollrechte der betroffenen Personen, wie etwa Informations- und Auskunftsrechte, enthält die Datenschutzgrundverordnung. Aber wie steht es mit der Umsetzung in der Praxis? Um dies näher zu untersuchen, hat die Stiftung Datenschutz bereits im Jahre 2016 unterschiedliche Projekte verglichen sowie die technischen, rechtlichen und ökonomischen Herausforderungen von „Personal Information Management Systeme“ (PIMS) geprüft und darauf basierend eine Studie mit dem Titel „Neue Wege bei der Einwilligung“[2] erstellt. Die untersuchten Konzepte beinhalteten unterschiedliche Herangehensweisen, um die Kontrollrechte der Nutzer·innen zu verbessern: Beispielhaft kann auf automatisiert generierte Auskunftsersuchen oder auf einen Dienst verwiesen werden, der eine Linksammlung zu den Privatsphäreeinstellungen unterschiedlicher Anbieter bereitstellte. Ein weiteres Projekt bot Unterstützung bei der Deinstallation von Apps an, die auf persönliche Daten zugreifen, während ein anderer Dienst die lokale Verwaltung persönlicher Daten auf dem eigenen Endgerät ermöglichte, die von unterschiedlichen Social Media Anbietern verarbeitet werden. Der Fokus dieser Projekte liegt auf dem Selbstdatenschutz, auf Verbesserung der Kontrollrechte der betroffenen Personen, unterstützt durch technische Lösungen. In diesem Zusammenhang ist darauf hinzuweisen, dass sich auch die Datenethikkommission in ihrem Abschlussbericht im Jahre 2019 für die Entwicklung innovativer Einwilligungsmodelle, wie z.B. PIMS, im Forschungskontext ausgesprochen hat.[3]

Einwilligung als praxistaugliche Rechtsgrundlage der Datenverarbeitung?

In dem rechtlichen Gutachten zur Studie der Stiftung Datenschutz[4] wurde die Frage behandelt, inwieweit eine Einwilligung automatisiert durch einen (digitalen) Assistenten erteilt werden könnte. Dies ist problematisch, da es aus rechtlicher Sicht spezifizierter bzw. eindeutiger Zwecke bedarf, die im Zeitpunkt der Erklärung transparent sein müssen. Eine Einwilligung muss informiert und freiwillig sein. Dennoch hat das Forschungsprojekt „Innovatives Datenschutz-Einwilligungsmanagement“[5], durchgeführt vom Institut für Verbraucherpolitik ConPolicy und gefördert vom Bundesministerium der Justiz und für Verbraucherschutz, nun gezeigt, dass es technische sowie gestalterische Möglichkeiten gibt, datenschutzfreund-

2 „Stiftung Datenschutz (2017): Neue Wege bei der Einwilligung, https://stiftungdatenschutz.org/themen/pims-studie/“

3 Datenethikkommission (2019): Gutachten, S. 126, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=1D9BFC866CEC7865662093BB1A47A221.1_cid287?__blob=publicationFile&v=6

4 Anne Riechert, Stiftung Datenschutz (2016): Stellungnahme zu rechtlichen Aspekten eines Einwilligungsassistenten, https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Stellungnahme_Rechtliche_Aspekte_eines_Einwilligungsassistenten_Anhang_1_final.pdf

5 Conpolicy (2020): Innovatives Einwilligungsmanagement, https://www.conpolicy.de/referenz/innovatives-datenschutz-einwilligungsmanagement/

liche Voreinstellungen entsprechend der Vorgaben der Datenschutzgrundverordnung (DSGVO) rechtskonform festzulegen. Die Studie hat zum einen ergeben, dass Verbraucher·innen differenzierte Einwilligungen und datensparsame Voreinstellungen überwiegend klar befürworten. Zum anderen konnte im Rahmen des gemeinsam mit Miele und der Deutschen Telekom durchgeführten Projekts ebenso eine praxistaugliche Lösung entwickelt werden.[6] Alles in allem wurde damit deutlich, dass die Kritik, welche die Praxistauglichkeit der Einwilligung infrage stellt, oftmals nicht gerechtfertigt ist. Betont wurde außerdem, dass Unternehmen durch die Bereitstellung von Wahlmöglichkeiten hinsichtlich der Einschätzung ihrer Vertrauenswürdigkeit sogar profitieren können.

Cookies und Privatsphäre als Standardeinstellung

Im ersten Entwurf zur ePrivacy-Verordnung[7] aus dem Jahre 2017 wurden Webbrowser als Torwächter bezeichnet und es wurden Hersteller in die Pflicht genommen, datenschutzfreundliche Webbrowser zu programmieren. Privatsphäre sollte zur Standardeinstellung werden. Diese Regelung wurde im Laufe der Verhandlungen zur ePrivacy-Verordnung in den Entwürfen der unterschiedlichen Ratspräsidentschaften gestrichen und unter portugiesischer Ratspräsidentschaft nun aktuell der Vorschlag unterbreitet, dass die Selbstbestimmung der Nutzer·innen vorgehen und Vorrang vor allgemeinen Softwareeinstellungen haben muss.[8]

Zu bedenken ist allerdings in diesem Zusammenhang, dass Selbstbestimmung nicht den datenschutzfreundlichen Voreinstellungen gegenübergestellt bzw. nicht in Widerspruch gesetzt werden sollte. Datenschutzfreundliche Voreinstellungen sollen gerade das Recht auf informationelle Selbstbestimmung, das Recht auf Schutz der personenbezogenen Daten sicherstellen, was dem Grundsatz „Datenschutz durch Technikgestaltung“ entspricht. Dies muss auch im Rahmen des Entwurfs zum Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) berücksichtigt werden.[9] So wurde die Frage aufgeworfen, ob ein Verbot von Browser-Voreinstellungen verankert werden sollte, die den Zugriff auf das Endgerät trotz entsprechender Einwilligung der Nutzer·innen verweigern. Hier stellt sich allerdings die technische Frage, wie ein Browser die Wirksamkeit einer Einwilligung automatisiert prüfen kann.

Fazit

Es gibt in der Praxis unterschiedliche Ansätze, um den Datenschutz für Nutzer·innen zu verbessern – sowohl mit Blick auf den Selbstdatenschutz als auch durch Konzepte, die es Unternehmen ermöglichen, Einwilligungen datenschutzkonform und durch verständliche Handhabung zu managen. Dieser Bereich sollte auch zukünftig intensiver erforscht werden. Der Grundsatz „Datenschutz durch Technikgestaltung“ spielt hierbei eine wichtige Rolle.

Prof. Dr. Anne Riechert ist seit 2016 wissenschaftliche Leiterin der Stiftung Datenschutz und Professorin für Datenschutzrecht und Recht in der Informationsverarbeitung an der Frankfurt University of Applied Sciences. Sie ist außerdem Vorstandsmitglied des Netzwerks AI Frankfurt Rhein-Main e.V. und stellvertretende Leiterin des Zentrums verantwortungsbewusste Digitalisierung (zevedi.de). Im vergangenen Jahr wurde Frau Riechert in den interdisziplinären „Beirat Beschäftigtendatenschutz“ des Bundesministeriums für Arbeit und Soziales (BMAS) berufen.

6 Zusammenfassung der zentralen Ergebnisse der Studie „Innovatives Einwilligungsmanagements (2020), https://www.bmjv.de/SharedDocs/Downloads/DE/News/PM/090720_Zusammenfassung.pdf?__blob=publicationFile&v=1

7 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010&from=DE

8 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10. February 2021, https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

9 Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien, https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/gesetz-zur-regelung-des-datenschutzes-und-des-schutzes-privatsphaere.html

PRIVATSPHÄRENSCHUTZ BEI DER NUTZUNG DIGITALER TECHNOLOGIEN UND SERVICES: DER GRUNDTON MACHT DIE MUSIK

Von Susen Döbelt, TU Chemnitz, und Frank Kienzle, secuvera GmbH

Privatsphäre beschreibt das Recht, allein gelassen zu werden, frei von Überwachung durch andere. Jede Person kann dieses, in unserer Gesetzgebung tief verankerte Recht, in der analogen Welt einfach und selbstbestimmt ausüben. Wir ziehen die Vorhänge zu, um uns vor neugierigen Blicken zu schützen. Wir verwahren ein Tagebuch an einem Ort, der für andere schwer zugänglich ist. Wir teilen vertrauliche Informationen nur mit bestimmten Personen, die wir gut kennen.

Bei der Nutzung digitaler Technologie und Services ist die Wahrung der Privatsphäre nicht so einfach zu realisieren. Welche Daten werden überhaupt bei der Nutzung erhoben und zu welchem Zweck? Welche Maßnahmen sind für den Schutz privater Informationen effektiv und wie setzt man sie ein?

Um diese Fragen zu beantworten, ist zum einen ein Problembewusstsein nötig, zum anderen ein gewisses Maß an digitaler Kompetenz. Für beides müssen die Nutzer·innen kognitive und zeitliche Ressourcen investieren, um Informationen wahrzunehmen, zu beachten, zu verarbeiten oder aus dem Gedächtnis abzurufen. Ob Maßnahmen wirksam sind, bleibt zudem oft unklar. Das Recht auf informationelle Selbstbestimmung wahrzunehmen, ist in der digitalen Welt für viele Nutzer·innen kaum zu bewältigen.

Um dies zu ändern, sollte Selbstdatenschutz ohne Hindernisse ermöglicht werden. Dabei ist eine Befähigung auf drei bekannten und miteinander verknüpften Ebenen notwendig.

Ebene 1: Transparenz.

Dies bedeutet, den Nutzer·innen Informationen zugänglich zu machen und diese so aufzubereiten, dass sie ein grundsätzliches Verständnis und den Aufbau eines mentalen Modells zu Datenflüssen und Funktionsweisen ermöglichen. Verständliche Formulierungen und Darstellungen können dazu beitragen.

Ebene 2: Kontrolle.

Hierzu ist es notwendig, zunächst Handlungsoptionen zu identifizieren, welche die Steuerung von datenschutzrelevanten Funktionsweisen ermöglichen. Anschließend müssen diese benutzerfreundlich gestaltet werden, so dass sie in den natürlichen Nutzungsablauf effizient und effektiv eingebettet sind. Passende Default-Einstellungen und Automatisierungsmöglichkeiten können dabei eine Umsetzung im (Nutzungs-)Hintergrund ermöglichen. (Push-)Benachrichtigungen oder Runtime-Abfragen stellen eine vordergründige Möglichkeit dar.

Ebene 3: Rückmeldung.

Informationen zu verschiedenen Handlungsoptionen und deren Effektivität und Konsequenzen können dazu beitragen, Nutzer·innen kurzfristig und langfristig zu motivieren, sich mit Selbstdatenschutz zu befassen. Numerische und/oder farbliche Kennzeichnung von Risiko oder Schutz der Nutzer·innen können dabei unterstützen.

Auf allen Ebenen gilt es, den kognitiven und zeitlichen Aufwand für die Nutzer·innen so gering wie möglich zu halten. Denn bei der Nutzung digitaler Technologien und Services stehen grundsätzlich andere Verhaltensintentionen als der eigene Datenschutz im Vordergrund: Primär möchten sich Nutzer·innen informieren, interagieren, oder bestimmte Aufgaben erledigen. Das Bedürfnis nach Datenschutz und Wahrung der Privatsphäre ist dabei ein individuell unterschiedlich ausgeprägter Wert, welcher „mitschwingt“. Mit anderen Worten, ein Grundton für die Musik „Nutzung digitaler Services und Technologien“.

Im Zuge der Europäischen Datenschutz-Grundverordnung wurden Hersteller und Anbieter rechtlich verpflichtet, Transparenz und Einstellungsmöglichkeiten zu schaffen. Dies führt aktuell dazu, dass Nutzer·innen mit langen, schwer verständlichen Texten und Einstellungsmöglichkeiten zu Beginn einer Nutzung konfrontiert werden. Die Möglichkeit zum Selbstdatenschutz gestaltet sich in der Praxis als Hindernis für die praktikable Nutzung.

Für die Ausgestaltung alltagstauglicher Möglichkeiten zum Selbstdatenschutz sind viele wissenschaftliche Disziplinen gefragt. So können Vertreter·innen aus der Informatik Informationen über Datenflüsse grundlegend erst einmal zugänglich machen sowie effektive Handlungsmöglichkeiten identifizieren oder schaffen. (Medien-)Psychologie, Medieninformatik und Interaktionsdesign können zur Informationsaufbereitung, Verständlichkeit und Effizienz beitragen. Disziplinen wie die (Medien-)Pädagogik können wertvolle Impulse für den Aufbau mentaler Modelle und Feedbackgestaltung geben.

Im BMBF-geförderten Forschungsprojekt PANDERAM erarbeiten wir interdisziplinär eine nutzerzentrierte Lösung für den Smartphone- und App-Bereich. Ziel des Projektes ist es, durch Bereitstellung von aufbereiteten Informationen zu App-Verhalten und Plattformsicherheit, Transparenz über Risiken für Nutzer·innen zu schaffen. Zudem sollen Handlungsoptionen in Form von datenschutzfreundlichen App-Alternativen zur Verfügung gestellt werden. Mittels einer Risikoanzeige wird Rückmeldung über die Effektivität getroffener Maßnahmen ermöglicht werden. Damit wollen wir die Nutzer·innen beim Wahrnehmen und Ausüben von Selbstdatenschutz im mobilen Kontext unterstützen: im Einklang mit den eigenen Bedürfnissen und möglichst frei von (Nutzungs-)Dissonanzen.

Susen Döbelt ist seit 2013 wissenschaftliche Mitarbeiterin an der TU Chemnitz. Aktuell ist sie an der Professur für Allgemeine Psychologie I und Human Factors im Rahmen des BMBF-geförderten Forschungsprojektes „PANDERAM: Privatsphären-Analyse und Nutzerspezifische Datenschutz-Empfehlungen für Apps und Mobilgeräte“ beschäftigt und hier für die Nutzerforschung verantwortlich. Ihre Forschungsschwerpunkte sind die nutzerzentrierte Gestaltung von privatsphärenschützender Technologie im Kontext Smartphone-Apps. Zudem forschte sie im Rahmen nationaler und europäischer Drittmittelprojekte zu Smart Grids, Peer-to-Peer Energy Management sowie im Bereich intelligentes Laden von Elektrofahrzeugen.

Frank Kienzle ist IT-Sicherheitsberater und Penetrationstester bei secuvera. IT-Sicherheit als elementare Voraussetzung für Privatsphäre im Digitalen war und ist seine Motivation nach dem Elektrotechnik-Studium in der IT-Security zu arbeiten. Im Projekt PANDERAM arbeitet er mit daran, auch Durchschnittsanwendern eine selbstbestimmte und datensparsame Nutzung von Smartphones zu ermöglichen.

IT'S THE DEVELOPERS!

Von Dr.-Ing. Frank Pallas, TU Berlin,
Information Systems Engineering[10]

Datenschutz muss technischer werden und sich die Gegebenheiten moderner Systementwicklung zu eigen machen. Dies gilt insbesondere auch für Datenschutzerklärungen, die ihren eigentlichen Zweck heute nicht mehr erfüllen.

Von breiten, unspezifischen Einwilligungen bis zu kaum verständlichen Datenschutzerklärungen: Die gelebte und täglich erlebte Praxis des Datenschutzes ist in vielerlei Hinsicht unbefriedigend und erfüllt die dem Datenschutzrecht eigentlich zu Grunde liegenden Ziele oftmals nicht (mehr) bzw. nur (noch) unzureichend.

Beispielhaft wird dies an Datenschutzerklärungen, wie wir sie heute „in the wild" vorfinden, deutlich. Ihrem ursprünglichen Zweck – einzelnen Bürger·innen auf Basis transparenter Informationen selbstbestimmt-souveräne, wohlinformierte Entscheidungen z.B. zur Nutzung eines Dienstes zu ermöglichen – werden sie in heute üblichen Ausprägungen nicht mehr gerecht. Sie sind zu lang, um von den Betroffenen realistischerweise gelesen und rezipiert zu werden, in ihrer Komplexität und juristischen Sprache nicht ausreichend verständlich und in weiten Teilen zu diffus und unspezifisch (z.B. hinsichtlich der konkret erhobenen Daten und der damit verfolgten Zwecke), als dass sie ein wirklich informiertes und souveränes Handeln ermöglichen würden.

Der „modus operandi" des Datenschutzes ist oftmals dysfunktional

Viele derartige Dysfunktionalitäten lassen sich auf den „modus operandi" des Datenschutzes zurückführen. Bei Datenschutzerklärungen handelt es sich etwa im Kern – trotz allen technischen Fortschritts – immer noch um *(Text-) Dokumente*, die von den Betroffenen aufmerksam zu *lesen* (und zu verstehen) sind. In den Grenzen dieses bisherigen „modus operandi" werden sich die Unzulänglichkeiten der gelebten Datenschutzpraxis dabei naturgemäß kaum überwinden lassen: Ein Textdokument, das Informationen zur Datenerhebung und Verarbeitung ausreichend präzise und spezifisch darstellen soll, würde in vielen Fällen gezwungenermaßen nochmals länger und unübersichtlicher, als es heute ohnehin schon der Fall ist.

Datenschutz muss technischer werden – auch jenseits von Verschlüsselung und Anonymisierung

Technisch getriebene Ansätze – so genannte „Privacy Enhancing Technologies (PETs)" – auch jenseits bereits weit etablierter Verfahren zur Verschlüsselung, Anonymisierung etc. versprechen demgegenüber vollkommen neue Möglichkeiten. In der Wissenschaft werden zahlreiche Ansätze hierzu seit geraumer Zeit diskutiert. Das Feld existierender PETs reicht dabei vom technischen Einwilligungsmanagement über die technische Repräsentation und Aufbereitung von bislang in Datenschutzerklärungen bereitgestellten Transparenzinformationen bis zur technischen Umsetzung der datenschutzrechtlichen Zweckbindung. Auch regulatorische Vorgaben schreiben unter dem Stichwort „Privacy / Data Protection by Design" den praktischen Einsatz von PETs zunehmend vor. Wichtig hierbei ist, dass sich derartige Verpflichtungen auf alle Datenschutzprinzipien – also etwa auch auf das der Transparenz, der Zweckbindung oder der Einwilligung als Legitimationsgrundlage – beziehen.

10 https://www.ise.tu-berlin.de/fp

Dennoch haben sich PETs jenseits von Sicherheits- und Anonymisierungsverfahren bislang noch nicht in der Breite durchgesetzt. Dafür gibt es Gründe, die zu adressieren sind.

Die aufwandsarme praktische Umsetzbarkeit in der realen Systementwicklung ist für die tatsächliche Anwendung von PETs zentral

Bisher vorgeschlagene PETs zeichnen sich oftmals dadurch aus, dass sie den Gegebenheiten moderner Systementwicklung nicht ausreichend Rechnung tragen. Annahmen z.B. über genutzte Datenbanken, Schnittstellen, Architekturmodelle etc. stimmen etwa häufig nicht mit der Praxis überein und das Zusammenspiel zwischen vorgeschlagenen PETs und in der Realität maßgeblichen Technologien und Programmierframeworks ist oftmals das Gegenteil von „nativ". Ähnliches gilt für die schlüssige Integration in moderne, oft agile Entwicklungsprozesse, -methoden, und -werkzeuge. Auch hier ist es notwendig, dass vorgeschlagene PETs sich schlüssig und mit wenig Zusatzaufwand in diese einbetten.

Die rechtliche Verpflichtung zum Einsatz hängt zudem explizit vom jeweiligen Stand der Technik und von den für die Umsetzung notwendigen Aufwänden und Kosten ab. Hieraus ergeben sich drei Ansatzpunkte, um den Einsatz von PETs voranzutreiben und jedenfalls mit höherer Wahrscheinlichkeit auch verpflichtend zu machen:

1. PETs müssen als Teil des „Stands der Technik" in ausreichender Reife und für die in der Praxis relevanten Systemkomponenten zur Verfügung stehen.

2. Der Aufwand zur Integration einer PET in reale Systemarchitekturen und Entwicklungsprozesse muss möglichst gering sein. Hierzu müssen PETs sich explizit an diesen orientieren. Dies wiederum erfordert, von Beginn an die Perspektive derjenigen Entwickler·innen einzunehmen, die die realen Systeme bauen. Die konkrete Integration einer PET muss für diese Entwickler·innen möglichst aufwandsarm möglich sein.

3. Die durch PETs in realen Systemkontexten hervorgerufenen Kosten (z.B. für zusätzliche Ressourcen wegen aus der Technologie resultierender Performanceverluste) muss möglichst gering, zumindest aber grob bezifferbar sein.

Eine solche, explizite Fokussierung auf die Sicht derjenigen Entwickler·innen, von denen wir uns einen vermehrten praktischen Einsatz von PETs wünschen, wird für die tatsächliche, breite Etablierung von „Privacy / Data Protection by Design" entscheidend sein. An der TU Berlin haben wir in diversen Forschungsprojekten entsprechende Technologien etwa zum Einwilligungsmanagement, oder zur Zweckbindung entwickelt und zur freien Nutzung öffentlich bereitgestellt. Aktuell entwickeln wir im BMJV-geförderten Projekt DaSKITA[11] u.a. Verfahren zur maschinenlesbaren Repräsentation von Angaben aus Datenschutzerklärungen und zu darauf aufbauenden, neuen Transparenzansätzen. Unsere Erfahrungen hieraus stimmen uns für einen zukünftigen, breiten Einsatz von PETs in der Praxis durchaus positiv.

Dr.-Ing. Frank Pallas ist Senior Researcher im Fachgebiet Information Systems Engineering der TU Berlin. Er forscht und lehrt an der Schnittstelle von Datenschutz(recht) und konkreter informatischer Systemgestaltung („Privacy Engineering"). Ein besonderer Schwerpunkt liegt dabei auf neuen, praxistauglichen Technologien zur Adressierung von Datenschutzprinzipien jenseits von Datensparsamkeit und Sicherheit, wie etwa Zweckbindung oder Transparenz. Er ist Principal Investigator und Gesamtprojektleiter des BMJV-geförderten Projekts „Datensouveränität durch KI-basierte Transparenz und Auskunft (DaSKITA)".

11 https://daskita.github.io/

WIESO TRANSPARENZ NICHT AUSREICHT

Von Marit Hansen, Landesbeauftragte
für Datenschutz Schleswig-Holstein[12]
und Mitglied im Forum Privatheit[13]

Transparenz ist eine wichtige Grundlage für den Datenschutz. Doch bedeutet eine verständliche Information über Datenschutzaspekte noch nicht, dass die betroffenen Personen sich der mit der Verarbeitung verbundenen Risiken wirklich bewusst werden. Auch gewährleistet Transparenz keineswegs Rechtskonformität oder Fairness der Datenverarbeitung.

Transparenz als Datenschutzgrundsatz

Transparenz gehört zu den Datenschutzgrundsätzen, die in Artikel 5 der Datenschutz-Grundverordnung (DSGVO) formuliert sind. Anforderungen an Informationspflichten der Verantwortlichen und Auskunftsmöglichkeiten für die betroffenen Personen ziehen sich durch die gesamte DSGVO. Es geht nicht nur um die Bereitstellung von korrekten Informationen über die Datenverarbeitung, sondern dies muss „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ (Artikel 12 Abs. 1 DSGVO) geschehen.

12 https://www.datenschutzzentrum.de

13 https://www.forum-privatheit.de

„One size fits all“ leistet keine Verständlichkeit

Mit der Verständlichkeit ist es aber so eine Sache, besonders wenn die Datenverarbeitung komplex ist oder häufigen Änderungen unterliegt – und das ist der Normalfall bei einer agilen Systemgestaltung, die zudem Code-Komponenten und Dienstleistungen von anderen integriert. Auch Verfahren mit eingebautem Datenschutz weisen oft zusätzliche Komplexität auf, z. B. durch besondere Verschlüsselungskonzepte oder Verteilung der Daten und der Verarbeitung. Komplexe Sachverhalte sind jedoch nur schwer so zu vermitteln, dass sie für jede Zielgruppe verständlich sind. Die DSGVO verlangt daher auch eine zielgruppengerechte Aufbereitung der Informationen, die sich speziell an Kinder richten. Schon seit vielen Jahren empfehlen die Datenschutzbehörden der EU ein Mehrebenen-Format für Datenschutzerklärungen, das auf einen Blick die wichtigsten Informationen darstellt und Details für diejenigen bereithält, die Genaueres wissen möchten.[14] [15] Problem: Verschiedene Aufbereitungen in Sprache oder Bildern für dieselbe Datenverarbeitung sind nicht äquivalent, und selbst wenn sie es wären, würden Menschen mit unterschiedlichem Wissensstand zu Abläufen und Risiken einer Datenverarbeitung und mit ihren verschiedenen Erwartungen nicht dasselbe verstehen.

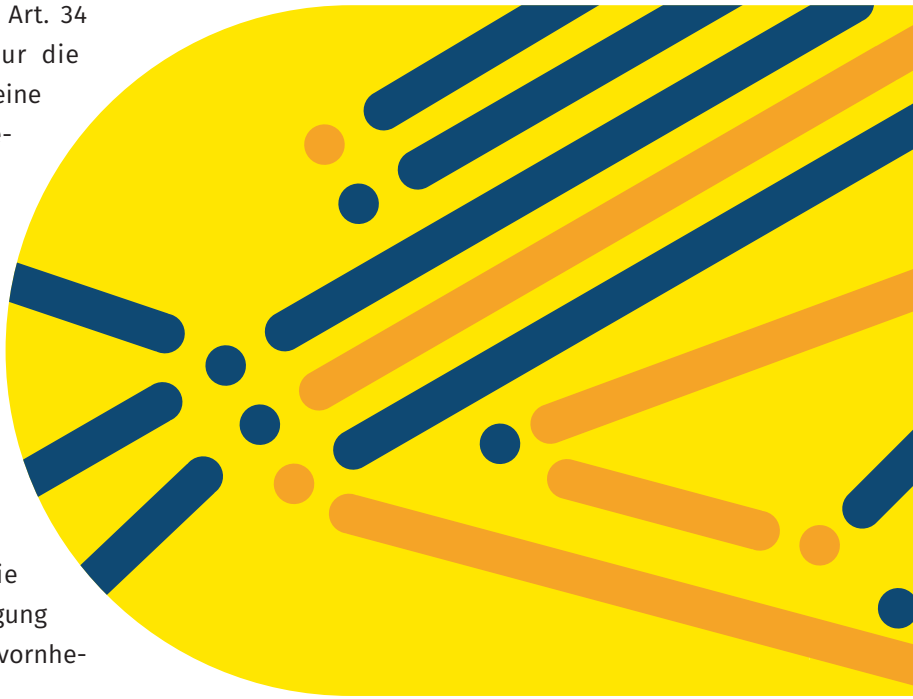
Framing durch die Verpackung der Informationen

Das Datenschutzrecht stellt zwar Anforderungen an die zu gebenden Informationen, aber regelt nichts zur „Verpackung“. So enthalten einige Benachrichtigungen von betroffenen Personen über eine Datenpanne,

14 Artikel-29-Datenschutzgruppe (2004): Stellungnahme 10/2004 zu einheitlicheren Bestimmungen über Informationspflichten, 11987/04/DE, WP 100, angenommen am 25. November 2004; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_de.pdf

15 Artikel-29-Datenschutzgruppe (2017): Leitlinien für Transparenz gemäß der Verordnung 2016/679, 17/DE, WP 260 rev.01, angenommen am 29. November 2017, zuletzt überarbeitet und angenommen am 11. April 2018; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

die bei voraussichtlich hohem Risiko nach Art. 34 DSGVO gegeben werden müssen, nicht nur die Pflichtinformationen, sondern lesen sich wie eine Wiedergutmachung, indem Gutscheine mitgesandt werden oder anders für das Unternehmen geworben wird. Einige Online-Shopping-Anbieter versenden bereits Entschuldigungs-E-Mails mit einem Gutschein, wenn ihr Server kurzzeitig ausgefallen ist, auch wenn der Ausfall noch nicht einmal eine meldepflichte Datenschutzverletzung darstellt. Passiert dann mal wirklich eine ernste Datenpanne, fällt dies weniger auf. Natürlich kann es auch sein, dass die betroffenen Personen ohne einen Mehrwert wie einem Gutschein den Inhalt der Benachrichtigung gar nicht als relevant einstufen, sondern von vornherein ignorieren würden.



Allenfalls diffuses Verständnis über Risiken und Folgen

Auch wenn neutral über die Datenverarbeitung informiert wird, kann es schwerfallen, aus den Informationen abzuleiten, welche Risiken bestehen und welche Folgen die Datenverarbeitung haben kann. Zum Beispiel enthalten die Informationen von Facebook zu Fanpages[16] einen Passus zu der Protokollierung von „Events“ bei der Interaktion von Personen mit Seiten oder Inhalten. In einer langen Liste werden Datenpunkte dieser Events beispielhaft aufgezählt: vom Starten einer Kommunikation bis hin zu Klicks oder Mouse-overs auf der Fanpage. Inwieweit die Auswertung der Events ein manipulatives Microtargeting[17] ermöglicht – beispielsweise durch auf die Nutzenden zugeschnittene Werbungen für Produkte oder um Wählerstimmen – und dass auf Basis der Daten passend zur jeweiligen Stimmung die passenden Inhalte mit musikalischer Untermalung präsentiert werden können, lässt sich aus einer technisierten Darstellung der Datensammlung nicht erahnen.

Risiken verdrängen und vergessen

Viele der Risiken sind ohnehin schwer einschätzbar, z. B. die Zugriffe von staatlichen Organisationen aus Ländern außerhalb des Europäischen Wirtschaftsraums, ohne dass für die europäischen Bürger·innen ein effektiver Rechtsschutz gegeben ist (s. a. EuGH-Urteil „Schrems II – C-311/18). Keine gute Lösung ist das Einholen von Einwilligungen in eine Datenverarbeitung nach einem Warnhinweis bezüglich der geheimdienstlichen Zugriffsmöglichkeiten in Take-it-or-leave-it-Situationen (was von Befürworter·innen auf Art. 49 DSGVO gestützt wird). Damit wird weder das Problem behoben oder eine Übergangslösung geschaffen, noch werden die Nutzer·innen über erfolgte Zugriffe informiert. Zumal neigen Menschen dazu, solche Warnungen zu vergessen. Ein Beispiel aus der Datenverarbeitung: Für Sprach-Bots am Telefon wird diskutiert, dass sie sich als Bot zu erkennen geben sollen, doch sind einige Systeme kaum mehr

16 Facebook (2021): Informationen zu Seiten-Insights, 2021; https://www.facebook.com/legal/terms/page_controller_addendum

17 Kurz/Dachwitz (2019): Microtargeting und Manipulation: Von Cambridge Analytica zur Europawahl, Bundeszentrale für politische Bildung, 02.05.2019; https://www.bpb.de/gesellschaft/digitales/digitale-desinformation/290522/microtargeting-und-manipulation-von-cambridge-analytica-zur-europawahl

von natürlicher Sprache eines Menschen unterscheidbar (einschließlich gelegentlicher Ähm-Laute), sodass eine mögliche Klarstellung zu Beginn des Telefonats in Vergessenheit geraten kann.[18]

Datengieriges Getrickse

Dass für bestimmte Services – beispielsweise bei einer Personalisierung – auch bestimmte personenbezogene Daten oder besondere Verarbeitungsschritte erforderlich sind, ist klar. Doch wenn man nur die Grundfunktionalität nutzen möchte, die mit einem geringeren Umfang an Daten und an Verarbeitungen auskommen müsste, geht dies in der Praxis häufig nicht: Die Wahlmöglichkeiten sind auf „Take it or leave it" beschränkt; das bedeutet in der Regel „Service gegen Daten". Oder die Nutzer·innen haben die Möglichkeit, bestimmte Verarbeitungen zu deaktivieren, aber dies wird ihnen durch die Nutzerführung nicht gerade leichtgemacht. Eine Gestaltung mit „Dark Patterns"[19][20] sorgt u. a. unter Ausnutzung psychologischer Tricks[21] dafür, dass die meisten Nutzer·innen doch keine datensparsamere Konfiguration einrichten.

Fazit

Transparenz allein gewährleistet offensichtlich nicht die Datenschutzkonformität der Datenverarbeitung. Auch führt eine Information über die Datenschutzaspekte nicht in jedem Fall dazu, dass sich die betroffenen Personen der für sie bestehenden Risiken bewusst werden.

Nach dem Verbraucherschutzrecht sind überraschende und versteckte Klauseln in den Allgemeinen Geschäftsbedingungen unwirksam, Verbraucherschützer·innen gehen regelmäßig gegen Tricksereien vor. Dies wird nun auch zu einer Aufgabe der Datenschützer·innen. Wesentlich wird sein, das Prinzip von „Datenschutz by Default" als Startpunkt einer jeden Datenverarbeitung flächendeckend einzufordern und Standards sowohl für Fairness der Verarbeitung als auch für eine zielgruppengerechte, verständliche Information zu etablieren.

Marit Hansen ist seit 2015 die Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das Unabhängige Landeszentrum für Datenschutz (ULD), die Datenschutzbehörde des nördlichsten Bundeslandes. Davor war die Diplom-Informatikerin sieben Jahre lang stellvertretende Landesbeauftragte für Datenschutz. Im ULD hat sie den Bereich der Projekte für technischen Datenschutz aufgebaut, in dem in Kooperation mit Forschung und Wissenschaft die Herausforderungen für die Gesellschaft durch die zunehmende Digitalisierung betrachtet und Lösungsvorschläge für eine grundrechtskonforme Gestaltung von Systemen erarbeitet werden.

18 Nickel (2018): Sprachassistenten: Gesetzesentwurf verlangt von Bots, sich als solche zu zeigen, Golem, 24.05.2018, https://www.golem.de/news/sprachassistenten-gesetzesentwurf-verlangt-von-bots-sich-als-solche-zu-zeigen-1805-134552.html

19 Forbrukerrådet (2018): Deceived by Design, Report, 2018; https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

20 Martini/Drews/Seeliger/Weinzierl (2021): Dark Patterns, Zeitschrift für Digitalisierung und Recht (ZfDR) 1/2021, 47-74

21 Acquisti/John/Loewenstein (2013): What Is Privacy Worth?, Journal of Legal Studies 42, no. 2 (June 2013): 249–274; doi:10.1086/671754; http://nrs.harvard.edu/urn-3:HUL.InstRepos:37101490

Digital
Autonomy Hub
Technik souverän nutzen

Der Digital Autonomy Hub – Technik souverän nutzen ist ein Kompetenzzentrum, das ein interdisziplinäres Netzwerk von 43 Instituten und Organisationen koordiniert. Der Hub macht sichtbar, woran die Partner forschen und welche Ideen sie entwickeln, um die individuelle digitale Souveränität zu stärken. Ziel dieses Wissenstransfers ist es, allen Menschen einen reflektierten und selbstbestimmten Umgang mit ihren Daten, Geräten und Anwendungen zu ermöglichen. Das Kompetenzzentrum bereitet aktuelle Forschungsergebnisse für Zivilgesellschaft, Politik, Wissenschaft und Wirtschaft auf und berät die verschiedenen Akteure zu ethischen, rechtlichen und sozialen Aspekten der Datennutzung.

Der Digital Autonomy Hub wird vom Bundesministerium für Bildung und Forschung im Rahmen des Forschungsprogramms „Technik zum Menschen bringen“ gefördert und von AlgorithmWatch und Gesellschaft für Informatik e.V. (GI) umgesetzt.

Mehr Informationen unter: www.digitalautonomy.net

(In-)transparente Datenschutzerklärungen und digitale Mündigkeit

Arbeitspapier des Digital Autonomy Hubs
April 2021

Veröffentlicht von

AW AlgorithmWatch gGmbH
Linienstr. 13, 10178 Berlin

Gesellschaft für Informatik e.V. (GI)
Spreepalais am Dom, Anna-Louisa-Karsch-Straße 2, 10178 Berlin

Kontakt: info@digitalautonomy.net

Layout: Beate Autering

Der Digital Autonomy Hub
wird gefördert vom

Bundesministerium
für Bildung
und Forschung

im Rahmen des Forschungsprogramms
„Technik zum Menschen bringen“