Transparenz & Datenschutz: Privacy Icons aus Sicht von UX Professionals

Workshop des German UPA-Arbeitskreises Usable Security & Privacy

Timo Jakobi
Universität Siegen
Siegen, Germany
timo.jakobi@uni-siegen.de

Mandy Balthasar
Universität der Bundeswehr München,
Germany
mandy.balthasar@unibw.de

Martina Borkowsky
McAfee, Schiphol-Rijk, Netherlands
Martina_Borkowsky@McAfee.com

Hartmut Schmitt
HK Business Solutions GmbH
Sulzbach, Germany
hartmut.schmitt@hk-bs.de

ZUSAMMENFASSUNG

Spätestens mit Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) sind die Themen Datenschutz und Umgang mit personenbezogenen Daten im Berufsalltag der Usability Professionals angekommen. Neben vielen anderen Prozessen sieht die DSGVO explizit die Entwicklung von Privacy Icons vor, um die Datenverarbeitung und -nutzung für die Betroffenen überschaubarer und einfacher erfassbar zu machen. Eines der wichtigsten Anwendungsgebiete stellen Datenschutzhinweise dar, die häufig nicht gelesen werden und damit eine „informierte Einwilligung“ fraglich erscheinen lassen.

In unserem Workshop nehmen wir die TeilnehmerInnen mit auf einen Design-Exkurs: Wir stellen Ergebnisse bisheriger Forschung vor, wie NutzerInnen über Privatheitsrisiken denken, und erweitern diese um die Perspektive professioneller UXlerInnen. Vor allem wird es kreativ und praktisch: In einem Hands-on wollen wir gemeinsam Lösungen für die wahrgenommenen Risiken in prototypische Designs überführen und diskutieren.

SCHLAGWORTE

Privacy, Datenschutz, Icons, Datenschutzhinweise, Privatheitsrisiken

Veröffentlicht durch die Gesellschaft für Informatik e.V. und die German UPA e.V. 2020 in H. Fischer & S. Hess (Hrsg.):
Mensch und Computer 2020 – Usability Professionals, 06.-09. September 2020, Magdeburg (remote)

https://doi.org/10.18420/muc2020-up-0384

1 Einführung

Mit der EU-Datenschutzgrundverordnung [10] gilt seit dem 25. Mai 2018 innerhalb der Europäischen Union ein einheitliches Datenschutzrecht. Ziel der DSGVO ist es, die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen, insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 DSGVO). Betroffen von der DSGVO sind alle Unternehmen, welche personenbezogene Daten erfassen, verarbeiten und speichern. Diese Unternehmen stehen vor der Herausforderung, praktikable und gleichzeitig benutzerfreundliche Lösungen zu finden, um rechtskonform mit der Identität von Kunden sowie mit deren Einwilligungen zur Verarbeitung personenbezogener Daten umzugehen. Denn bei Nichteinhaltung der DSGVO-Vorschriften drohen den Unternehmen sowohl empfindliche Bußgelder als auch strafrechtliche Sanktionen. Gleichzeitig ist auch ein möglicher Reputationsschaden nicht zu unterschätzen. Eine zentrale Eigenschaft der DSGVO liegt darin, viele neue und damit auch unklare Rechtsbegriffe einzuführen. Sie ist zudem technisch neutral – schreibt also bspw. keine Verschlüsselungstechnologien vor, sondern spricht eher von Schutzmaßnahmen nach dem Stand der Technik. Dies hat den Vorteil, dass die DSGVO mit der Zeit und der technischen Entwicklung mitwachsen kann. Auf der anderen Seite erwachsen durch diese vagen Formulierungen jedoch Unsicherheiten, bspw. bezüglich anzubringender Schutzmaßnahmen.

Auch für Usability- und User-Experience-Professionals (UUX-Professionals) spielt dies eine Rolle, denn sie sind oft maßgeblich am Design der interaktiven Systeme beteiligt, welche die DSGVO-konforme Verarbeitung personenbezogener Daten gewährleisten sollen. Prominente Beispiele für Schutzmaßnahmen sind die DSGVO-Prinzipien Privacy by Design und Privacy by Default (Art. 25 DSGVO), also die Gewährleistung von Datenschutz bzw. Datenminimierung durch eine entsprechende Ausgestaltung der Hard- und Softwarekomponenten sowie nutzerfreundliche Voreinstellungen. Die DSGVO führt jedoch auch viele neue Rechte für die Datensubjekte (=User) ein, deren Ausgestaltung im

Sinne der NutzerInnen Gegenstand der Forschung ist [1, 24]. Weiter führt die DSGVO in Artikel 12 Absatz 8 auch die Möglichkeit ein, europaweit einheitliche Icons, die Datenschutzinformationen kommunizieren sollen, zu implementieren. Diese könnten bspw. dazu beitragen, die von NutzerInnen geradezu chronisch ignorierten Datenschutzhinweise [17, 19] in Zukunft benutzerfreundlicher zu gestalten. An solchen Icons haben sich schon viele Initiativen versucht, aber keine hat sich durchsetzen können: Häufig waren dabei die Gestaltungsprozesse getrieben aus Richtung eines bestimmten Stakeholders, sei es als gestalterische Übung von Designern oder als Projekt aus Richtung des Verbrauchers. Eine wissenschaftlich umfassende Betrachtung der Bedarfe der unterschiedlichen Stakeholder und die Aushandlung teils konfligierender Zielinteressen fehlen bis dato. Daher wollen wir in diesem Workshop bereits eingeholte Privatheitsbedarfe und -risiken von NutzerInnen vernetzter Geräte heranziehen, um auf dieser Basis Skizzen für mögliche Icons zu gestalten, die den Bedarfen der NutzerInnen – eine Evaluation natürlich ausstehend – tatsächlich entsprechen könnten.

2 Interkulturelle Implikationen und Performanz für Icons

Zunächst ein kleiner Exkurs zur Nutzung und Bedeutung von Icons: Icons, welche als Grafik eine Information tragen, werden in wahrscheinlich allen Kulturen genutzt. Maßgeblich beeinflusst wird deren Gestaltung durch die zu vermittelnde Information, das Trägermedium sowie die zu erreichenden EmpfängerInnen. Somit steht der künstlerische Aspekt des Icons weniger im Vordergrund, wobei die Interpretierbarkeit eines Icons als Grafik oder auch als Kunst keine harte Grenzziehung ermöglicht. Verhältnismäßig schnell geklärt sind in Bezug auf Privacy die Fragen nach der zu vermittelnden Information bzw. auch nach dem Trägermedium. Wobei die Zielsetzung der Vermittlung dieser komplexen Inhalte durch eine Visualisierung alles andere als trivial ist. Sachverhalte zu vermitteln, welche Orientierung bieten und dabei keine Fehlinterpretationen zulassen, ist bereits eine Herausforderung. Hinzukommt jedoch häufig ein reizüberflutendes Umfeld, welches bereits einen Großteil der Aufmerksamkeit auf sich zieht. Und auch der dritte Aspekt, die EmpfängerInnen, welche die optimale Informationsdichte präsentiert bekommen sollen, bringen bereits einiges an kulturell zu berücksichtigendem Kontext mit. Informationsdichte bzw. Informationsfrequenz wurden im Rahmen einzelner Dimensionen der Mensch-Computer Interaktion für den interkulturellen Kontext bereits umfassend aufbereitet [12]. Dabei dreht es sich beispielsweise um Farben, Formen, Symbole oder auch die Leserichtung, welche die Wahrnehmung und das Denken prägen. Bei all diesen Anforderungen, welche auch an Privacy Icons gestellt werden müssen, gilt es, sich von Beginn an ein „Erklärziel“ [28] zu setzen und sich auf diesen speziellen Sachverhalt zu konzentrieren.

Da jede Kultur sehr komplex ist, kann beispielsweise auch nicht auf *die* asiatische Kultur oder *die* westliche Kultur Bezug genommen werden. Es ist jedoch möglich, bestimmte kulturspezifische Gestaltungsmerkmale herauszuarbeiten, welche Gemeinsamkeiten sowie Unterschiede zwischen Ost und West aufzeigen. So kann festgehalten werden, dass in der Art und Weise des Denkens unterschieden werden kann. Menschen, welche durch eine Kultur mit einer mehrheitlich holistischen Denkweise geprägt sind, wie dies in vielen östlichen Ländern der Fall ist, werden ihre Aufmerksamkeit nicht allein auf das Icon legen, sondern auch auf den dahinterliegenden Kontext sowie mögliche Beziehungen zwischen weiteren Icons oder ergänzenden Informationen. BetrachterInnen eines Icons aus einem eher analytisch denkenden Kulturraum wie Europa oder den USA werden hingegen mehrheitlich die Eigenschaften eines Icons fokussieren [20]. Diese Art und Weise der Wahrnehmung und Interpretation gilt es bei der Erarbeitung von Privacy Icons zu berücksichtigen, um deren Bedeutung universell verständlich werden zu lassen.

Einfluss nehmen jedoch nicht nur die Traditionen einer Kultur, sondern auch die bis heute gepflegten Standards in Bezug auf die Nutzung von Grafiken. So geben beispielsweise im japanischen Kulturraum kleine Infografiken oder auch Icons auf behördlichen Formularen oder Gebrauchsanweisungen ganz selbstverständlich erklärende Hinweise. Weiter entstand in allen Kulturen, aufgrund von Verschmelzungen aus Tradition und Moderne, jeweils eine eigene Ästhetik. Beispielhaft kann hier genannt werden die Reduktion von Farbe im japanischen Design im Gegensatz zum eher als bunt zu bezeichnenden Ansatz im chinesischen Sprachraum. Aufgrund eines ganz wesentlichen Unterschiedes darf neben der Symbolbedeutung auch das Alphabet nicht vergessen werden. Das Bild, welches ein asiatisches Schriftzeichen abgibt, ist ein anderes als der Buchstabe eines römischen Alphabets. Aber auch der Vergleich eines schlichten Designs gegenüber einem Icon mit einer hohen Dichte an bedeutungsvoller koreanischer Ornamentik verdeutlicht Unterschiede in der Gestaltung von Informationen [28].

Trotz der dargelegten Unterschiede, kann festgehalten werden, dass ein Prozess der Transkulturalität auch in Bezug auf Icons Einzug hält. Aufgrund global steigender Vernetzungsdichte entwickelt sich auch ein kulturspezifisches Bewusstsein, welches sich unweigerlich auch im Design widerspiegelt [21]. So beispielsweise bei internationalen Icons für Flughäfen, welche auch in der internationalen technischen Dokumentation Gegenstand der Betrachtung sind. Wobei die DIN EN 82079-1 diese visuelle Anleitung zwar unterstützt, dennoch aber die Notwendigkeit der Erstellung einer eigenen Norm bzw. eines Normenabschnitts für die visuelle Gebrauchsanleitungen ergänzt werden müsste [6].

3 Privacy Icons als Lösungsansatz für Datenschutzhinweise in einer vernetzten Gesellschaft

Datenschutzhinweise werden oft nicht gelesen oder sind nicht gut lesbar [19]. Sie sind voll mit juristischem Jargon, der aus Sicht von NutzerInnen vielseitig interpretierbar ist und dadurch Unsicherheiten zur tatsächlichen Bedeutung von Ausdrücken und zur Verwendung von Daten hervorruft [18, 25].

Als eine Ergänzung zur besseren Lesbarkeit und Standardisierung von Datenschutzhinweisen existiert schon lange die Idee, Icons zu nutzen. Da alle Icons bisher jedoch auf der Freiwilligkeit von Dienstanbietern basieren, hat sich noch kein Modell praktisch durchsetzen können.

Die Datenschutzgrundverordnung hat in diesem Hinblick noch einmal einen neuen Impuls gegeben, denn sie sieht vor, dass die Europäische Kommission bemächtigt ist, standardisierte Icons für Datenschutz europaweit verpflichtend zu machen.

Transparenz durch Icons: Was sagt die DSGVO?

Die DSGVO setzt die Rahmenbedingungen für die Verwendung von Privacy Icons. Nach Artikel 12 Absatz 1 DSGVO muss derjenige, der für die Verarbeitung personenbezogener Daten verantwortlich ist die betroffenen Personen über die Verarbeitung informieren, und zwar „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“. Dies gilt für einen Plattformbetreiber, der personenbezogene Daten seiner NutzerInnen erhebt, speichert oder übermittelt, aber auch für Usability-TestleiterInnen, die Daten von ProbandInnen verarbeiten. Welche Daten hierbei als personenbezogen anzusehen sind, ist abhängig vom Verwendungszusammenhang. Neben dem Namen und der Anschrift können dies beispielsweise die IP-Adresse, ein Foto, ein Video, ein Fingerabdruck, das Geschlecht oder die Augenfarbe sein.

Die Informationen über die Verarbeitung der personenbezogenen Daten können nach Artikel 12 Absatz 7 DSGVO in Kombination mit standardisierten Bildsymbolen – sprich: mit Privacy Icons – bereitgestellt werden, „um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln“. Werden solche Bildsymbole in elektronischer Form dargestellt, müssen sie zudem maschinenlesbar sein. Hierdurch eröffnet die DSGVO Möglichkeiten der Automatisierung. Beispielsweise kann die Datenschutzrichtlinie eines Anbieters, die in Form von standardisierten Icons dokumentiert ist, ausgelesen und mit den Datenschutzpräferenzen einer Nutzerin abgeglichen werden; auf dieser Grundlage kann eine automatisch eine Einwilligung erteilt bzw. abgelehnt werden oder es können einzelne Einstellungen geändert werden.

Ferner wurde der Europäischen Kommission durch Artikel 12 Absatz 8 DSGVO die Befugnis übertragen, delegierte Rechtsakte zu erlassen, welche Informationen durch Bildsymbole darzustellen sind und welche Verfahren für die Bereitstellung standardisierter Bildsymbole zu verwenden sind. Nach Artikel 70 Absatz 1 Buchstabe r DSGVO soll der Europäische Datenschutzausschuss hierbei eine beratende Funktion einnehmen.

Ein Vorschlag zur DSGVO [3], der am 12.03.2014 vom Europäischen Parlament angenommen wurde, enthielt in „Anhang 1 – Darstellung der Hinweise nach Artikel 13a (neu)“ Entwürfe für sechs Privacy Icons, vgl. Beispiel in Abbildung 1. Diese Icons waren Teil eines umfassenderen Konzepts, mit dem die betroffenen Personen über bestimmte Sachverhalte beim Umgang mit ihren personenbezogenen Daten informiert werden sollten: „Erhebung“, „Aufbewahrung“, „Verarbeitung“, „Weitergabe“, „Verkauf und unentgeltliche Überlassung“ sowie „Verschlüsselung“ der Daten.

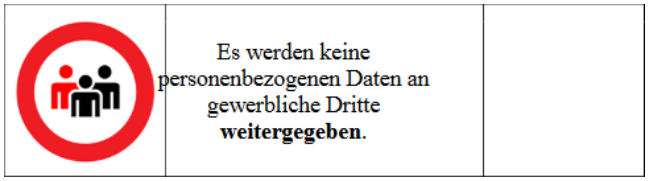

Abbildung 1: Icon-Entwürfe DSGVO (Beispiel “Weitergabe”)

Diese Information sollte in standardisierter Form erfolgen, bevor die Betroffenen ihre personenbezogenen Daten bereitstellen. Das Konzept sah eine dreispaltige Tabelle mit diesem Aufbau vor: Spalte 1 „Symbol“ – jeweiliges Privacy Icon; Spalte 2 „Wesentliche Informationen“ – vordefinierte Erläuterung zum jeweiligen Sachverhalt; Spalte 3 „Erfüllt“ – Piktogramm, mit dem angezeigt wird, ob der betreffende Hinweis für den jeweiligen Anbieter zutrifft oder nicht (grüner Haken bzw. rotes Kreuz, vgl. Abbildung 2). Der Vorschlag sah vor, dass die Proportionen der (gesamten) Tabelle und der Icons eingehalten werden, auch wenn die Tabelle verkleinert oder vergrößert wird.

Abbildung 2: Icon-Entwürfe DSGVO "ERFÜLLT"

Die Bewertungen dieses Konzepts und insbesondere des Icon Sets fielen ernüchternd aus: In einem Blogbeitrag aus datenschutzrechtlicher Sicht [26] wurde insbesondere das Verschlüsselungssymbol kritisiert, da dessen Hinweistext ausschließlich darauf abzielte, ob personenbezogene Daten verschlüsselt gespeichert werden, die ebenso wichtige Verschlüsselung des Transportwegs jedoch nicht thematisierte. Zudem wurde bemängelt, dass die Icons bzw. die damit verbundenen Aussagen keine Abstufungen zuließen – ein bestimmter Sachverhalt ist erfüllt beziehungsweise nicht erfüllt. Insgesamt wurden die Icons als zu schwer verständlich und nicht selbsterklärend eingeschätzt, insbesondere ohne die Hinweistexte. Weitere Punkte, die in den Kommentaren des Blogbeitrags angemerkt wurden, betrafen vor allem die grafische Gestaltung, die der Optik von Straßenverkehrsschildern nachempfunden war: das Icon-Set verwende teilweise die falsche Art von Schildern, nämlich Verbotszeichen statt Gefahrzeichen. Zudem hätten die Verbotsschilder eine negative, abschreckende Wirkung auf die NutzerInnen. Auch bei Anbietern, die die höchsten Datenschutzstandards erfüllen, würde diese Wirkung kaum durch entsprechende grüne Haken (Anforderungen sind erfüllt) kompensiert werden.

Von der Universität Karlstad wurde eine Kurzevaluation [22] durchgeführt, die aus drei Aufgaben bestand. Bei Aufgabe 1 sollten die TeilnehmerInnen (n=21), ohne die entsprechenden Hinweistexte zu kennen, versuchen, die Bedeutung der Icons zu beschreiben. Hier gab es nur wenige Übereinstimmungen. Beispielsweise enthält das Icon zum Hinweis „Es werden nicht mehr personenbezogene Daten erhoben, als für die spezifischen Zwecke der Verarbeitung erforderlich sind" eine Lupe, die über einer Person schwebt; dies wurde von den TeilnehmerInnen eher mit „Personensuche" oder „Detailinformationen" assoziiert. Die intendierte Bedeutung der Verbotsschilder-Optik (roter Kreis bedeutet Verneinung) wurde nur von einer Person richtig interpretiert. Bei Aufgabe 2 sollten die TeilnehmerInnen die sechs Icons den richtigen Hinweistexten zuordnen. Hier gelangen den 21 TeilnehmerInnen insgesamt 70 Übereinstimmungen (Ø 3,33). Bei Aufgabe 3 sollten die TeilnehmerInnen die Bedeutung einer vollständigen Tabellenzeile (Privacy Icon, Legende und Bewertungshinweis) beschreiben. Trotz der angegebenen Informationen – personenbezogene Daten werden nicht zu anderen als den Zwecken verarbeitet, für die sie erhoben wurden – waren fünf Befragte dazu nicht in der Lage, zehn Befragte dehnten die Bedeutung auch auf die Übermittlung von Daten aus. Zusammenfassend kam die Studie daher zu dem Schluss, dass die TeilnehmerInnen weder das grafische Schema des Gesamtkonzepts noch die einzelnen Icons verstanden.

In der heute gültigen Form der DSGVO sind diese Icon-Vorschläge oder eine überarbeitete Version des Icon Sets nicht mehr enthalten. Zudem fehlen verbindliche Vorgaben für die Verwendung von Privacy Icons. In der Praxis ist dadurch eine gewisse Verunsicherung entstanden: Verschiedene Websitebetreiber und Plattformen haben ihre Datenschutzrichtlinien mit selbstentwickelten Privacy Icons angereichert. Andererseits gibt es auch Stimmen [16], die von der Verwendung von Privacy Icons generell abraten, solange die EU-Kommission noch keine Klarheit geschaffen hat. Die Artikel 29-Gruppe, die bis Mai 2018 unabhängiges Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes war, vertrat die Auffassung [2], dass im Mittelpunkt der Entwicklung einer Bildsymbolregelung ein auf Fakten gestützter Ansatz stehen sollte. Im Vorfeld der Standardisierung sollten gemeinsam mit der Industrie und der breiten Öffentlichkeit umfangreiche Untersuchungen zur Wirkungskraft von Bildsymbolen durchgeführt werden.

In Deutschland versuchen sowohl staatliche Stellen als auch Nichtregierungsorganisationen darauf hinzuwirken, dass die Kommission möglichst rasch von ihrer Befugnis Gebrauch macht, delegierte Rechtsakte zur Verwendung standardisierter Bildsymbole zu erlassen. In jüngster Vergangenheit gab es entsprechende Initiativen beispielsweise vom Bundesrat [7] sowie von der Digitalen Gesellschaft e.V. und der Verbraucherzentrale Bundesverband [9]. Durch die EU-weite Vereinheitlichung bei der Verwendung von Privacy Icons erhofft man sich ein hohes Potential an Vereinfachung und eine Stärkung der NutzerInnen in ihren Grundrechten.

Privacy Icons in der Wirtschaft

Große internationale Plattform-Anbieter wie Google, Facebook oder Microsoft haben bereits vor dem Wirksamwerden der DSGVO-Regelungen damit begonnen, ihren NutzerInnen Möglichkeiten zur Verfügung zu stellen, mit welchen sie den Schutz ihrer Daten selbst verwalten können. NutzerInnen dieser Plattformen wird nun ermöglicht, mittels des Dashboards einzustellen, welche Daten die Plattformanbieter speichern beziehungsweise auswerten dürfen (z. B. Bewegungsprofile, Produktinteressen, Suchanfragen oder Kommunikationsdaten), aber auch welche Informationen für andere NutzerInnen sichtbar sind. Von verschiedenen Seiten wird jedoch kritisiert, dass diese Dashboards oft schwer zu finden und an sich zweischneidig sind, indem sie NutzerInnen verführen können, mehr Daten freizugeben [8].

Facebook hat nach einer Reihe von Berichten über unangebrachte Datenpraktiken ebenfalls damit begonnen, die Verbesserung der Datensicherheit und Privatsphäre voranzutreiben. Dabei wurden zunächst die Einstellungen zur Sicherheit und Privatsphäre komplett überarbeitet, sodass die NutzerInnen nun umfassendere Informationen zur Konfiguration ihrer persönlichen Einstellungen, zur Account-Sicherheit und zur Nutzung ihrer personenbezogenen Daten erhalten.

Google bietet seinen KundInnen eine Transparenzschnittstelle an, mit deren Hilfe diese in die Lage versetzt werden, getätigte Suchanfragen, Standortverläufe usw. einzusehen und zu löschen. Zusätzlich stellt Google einen Privatsphärecheck[1] zur Verfügung, einen Wizard, mit dem die eigenen Einstellungen zur Privatsphäre für den gesamten Google-Account verwaltet werden können.

Das Recht auf Datenübertragbarkeit gem. Artikel 20 DSGVO erfüllt Google mit dem Onlinedienst Google Takeout.[2] Dieser Dienst ermöglicht es registrierten Google-NutzerInnen, eine Kopie ihrer personenbezogenen Daten aus den von ihnen verwendeten Google-Diensten, wie beispielsweise Gmail, Google Kalender oder Google Fotos, zu exportieren. Die gewünschten Daten können ausgewählt und in gängigen Archivformaten wie JSON, CSV, HTML oder mbox heruntergeladen werden. Dadurch bietet sich registrierten NutzerInnen die Möglichkeit, ihre Daten zu sichern oder für die Nutzung in einem anderen Dienst zu verwenden.

In einer aktuellen Studie [23] wurden knapp zehn bekannte Social-Media-Anbieter und vergleichbare Plattformen in Bezug auf ihre Stärken und Schwachpunkte hinsichtlich des Datenschutzes analysiert. Das Ergebnis: Die Einstellungsmöglichkeiten sind oft versteckt. Zudem werden NutzerInnen häufig mit schwammigen Formulierungen und „Wohlfühltexten", die Datenschutz suggerieren („Ihre persönlichen Daten sind bei uns sicher …", „Wir verdienen uns Ihr Vertrauen Tag für Tag …"), in einer vermeintlichen Sicherheit gewogen [18, 25]. Die Voreinstellungen entsprechen oft nicht dem Privacy-by-Default-Prinzip, beispielsweise bei der Sichtbarkeit von Profilen oder Beiträgen. Auch erlauben die Voreinstellungen meist die Nutzung der Daten für personalisierte Werbung, Tracking oder Gesichtserkennung, aber auch für die Nutzung

[1] https://myaccount.google.com/intro/privacycheckup?hl=de

[2] https://takeout.google.com/

durch Drittanbieter, Einblendung des Profilbilds in Werbeanzeigen und Ähnliches. Ebenfalls als problematisch ist anzusehen, dass viele Plattform-Anbieter auch außerhalb ihres Netzwerks Daten erfassen. Zudem werden häufig Funktionen angeboten, durch die möglicherweise die Privatsphäre Dritter verletzt wird, beispielsweise die Möglichkeit eines Adressbuch- oder Kalenderabgleichs. Hier können Icons dazu beitragen, Unklarheiten abzubauen und zu einer stärker nutzerfreundlichen Ausgestaltung von Datenschutzhinweisen zu gelangen.

4 Risikobasierte, nutzerzentrierte Forschung

Bekanntermaßen verhalten sich NutzerInnen online häufig nicht in Übereinstimmung zu ihrer Einstellung zu Datenschutz. Für minimale Vorzüge, wie beispielsweise mehr Beachtung eines Fotos in sozialen Netzwerken, geben die NutzerInnen bereitwillig persönliche Daten preis. Dieses Phänomen ist allgemein als "Privacy Paradox" bekannt [4, 14].

Die Gründe für dieses Verhalten sind bereits mehrfach untersucht worden, aber bis heute unklar. Während manche – auch und gerade im Rechtsbereich bspw. unter dem Schlagwort der „informierten Einwilligung“ – von einer rationalen Entscheidung ausgehen, in welcher die NutzerInnen Kosten und Nutzen der Datenfreigabe gegeneinander abwägen [27], wird in zahlreichen Studien Gegenteiliges beobachtet.

Die Entscheidung zur Freigabe persönlicher Daten basiert in vielen Fällen auf der reinen Betrachtung des eigenen Vorteils und Nutzens, wobei die Risiken wenig oder gar nicht bedacht werden [29]. Das Erreichen des gewünschten Ziels lässt Risiken kleiner erscheinen, als sie sind, oder diese werden nicht weiter beachtet. Selbst bei angewandter Nutzen-Kosten-Analyse werden häufig Verhalten beobachtet wie eine Über- oder Unterschätzung der tatsächlichen Risiken oder Vorzüge. Die Tatsache, dass die NutzerInnen wenig bis keinerlei Wissen über *tatsächliche* Risiken haben, führt ebenfalls zu unüberlegten Entscheidungen, bei denen die persönlichen Vorzüge im Vordergrund stehen [5]. Dennoch hat sich gezeigt, dass Verbraucher in der Überlegung Daten freizugeben, Risiken als mögliche Gründe gegen eine Freigabe artikulieren und diese auch als Entscheidungsgrundlage nutzen, wenn sie ihnen präsentiert werden [11, 13, 15]. Nicht zuletzt eignet sich dieser Ansatz, da er sowohl im Bereich Usable Privacy, aber auch in der Regulation bekannt ist.

So kommt dem risikobasierten Ansatz bei der angemessenen Gestaltung von Icons der Risikowahrnehmung von VerbraucherInnen eine wichtige Rolle zu. Im Projekt „Privacy Icons“[3] des Lehrstuhls Digitale Selbstbestimmung am Einstein Center for Digital Future werden Datenschutz Icons in einem umfassenden, nutzerzentrierten Multi-Stakeholder-Gestaltungsprozess erforscht. Die wahrgenommenen Risiken wurden von NutzerInnen erfasst, mit RechtsexpertInnen abgeglichen und entsprechend kategorisiert. Auf Basis dieser Risiken und Kategorien sollen nun erste Grundlagen für Icons entstehen, die NutzerInnen ihrerseits als Inspiration und Ausgangslage für mögliche Lösungen heranziehen können sollen.

5 Workshop des Arbeitskreis Usable Security & Privacy der German UPA

Im Workshop wird aufgrund der oben aufgezeigten Herausforderungen ein Ansatz vorgestellt, mit dem Implikationen von Datenfreigaben durch Orientierung an von NutzerInnen wahrgenommenen Risiken verständlicher und zugänglicher kommuniziert werden. Durch diesen Ansatz sollen AnwenderInnen sowie Unternehmen in die Lage versetzt werden,

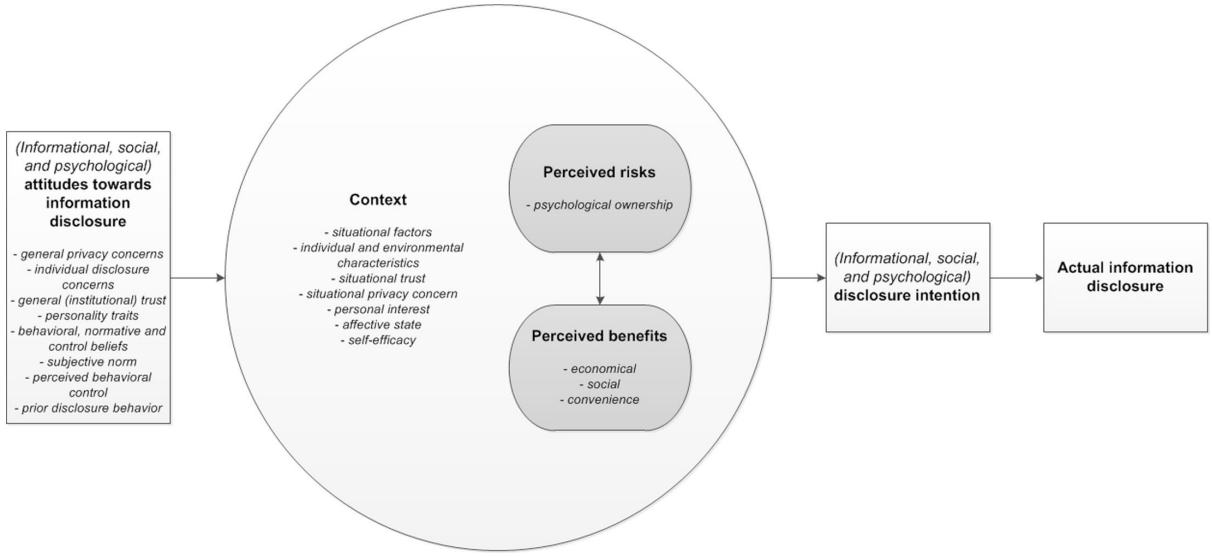

Abbildung 3: Überblick über die Variablen, die bei der von der Rationalität geleiteten Risiko-Nutzen-Kalkulation eine Rolle spielen [Barth & de Jong, 2017].

[3] https://privacy-icons.info

souverän mit ihren personenbezogenen Daten umgehen zu können, weil die bereitgestellten Icons an die Lebenswelt der NutzerInnen anknüpfen, indem konkrete Risiken – auch(ausgeschlossene Risiken – angemessen kommuniziert werden.

Ausgangspunkt werden von NutzerInnen wahrgenommene und artikulierte Risiken und ein Kategorisierungsvorschlag sein. Diese werden zunächst vorgestellt und diskutiert. Dann sollen je nach Vorliebe der TeilnehmerInnen entweder eigene Kategorienbäume aufgebaut werden oder alternativ Icons kreativ gescribbelt und diskutiert werden. Damit soll einerseits UX-Professionals demonstriert werden, welche Schutzbedarfe Menschen in der Freigabe von Daten artikulieren. Andererseits soll die gesammelte Erfahrung der UX-Community genutzt werden, um deren Ideen in erste Gestaltungsansätze zu überführen und so die Perspektive der NutzerInnen und der Rechtswissenschaft zu ergänzen. Die Ideen und Gestaltungsansätze können wiederum NutzerInnen zurückgespielt und damit einer Rückkopplung und Evaluation zugeführt werden.

6 Agenda des Workshops

Im Rahmen des 90-minütigen Workshops wird ein Erfahrungsabgleich mit den Teilnehmenden zu folgenden Themen durchgeführt:

- Einführung in DSGVO und Icons
- Vorstellung bestehender Privacy Icons und deren Perspektiven
- Vorstellung und Kategorisierungen von Risiken die NutzerInnen artikuliert haben.
- Kreativitätsphase: Prototyping/Scribbling von möglichen Icons und kurze abschließende Vorstellung

Außerdem werden im Rahmen des Workshops der Arbeitskreis Usable Security & Privacy, seine Themen, Ziele und Akteure sowie deren Projekte kurz vorgestellt. Die Hauptzielgruppe des Workshops sind UUX-Professionals, welche selbst beruflich im Themenumfeld Usable Security & Privacy aktiv sind bzw. eventuell in Zukunft sein werden. Der Workshop ist aber auch geeignet für interessierte EinsteigerInnen, die sich über die Themen Datenvisualisierung, Data Literacy, Usable Security & Privacy oder die Arbeit des Arbeitskreises informieren möchten. Die Ergebnisse des Workshops werden im Nachgang in einer geeigneten Form aufbereitet und den TeilnehmerInnen zur Verfügung gestellt bzw. veröffentlicht.

7 Arbeitskreis Usable Security & Privacy der German UPA

Der Arbeitskreis Usable Security & Privacy beschäftigt sich seit 2015 mit Ansätzen und Konzepten, welche sicherheits- und/oder privatheitsfördernde Verfahren für Software und interaktive Produkte stärker an den Zielen und Aufgaben der NutzerInnen ausrichten und welche dafür sorgen, dass Funktionsweisen von Sicherheitselementen auch für NichtexpertInnen verständlich gemacht werden. Ziel des Arbeitskreises ist es dabei, sowohl bei UUX-Professionals als auch bei NutzerInnen im privaten und beruflichen Umfeld ein verstärktes Bewusstsein für das Themengebiet Usable Security & Privacy zu schaffen.

Um die Arbeit der UUX-Professionals zu unterstützen, wird das vorhandene Fachwissen aus wissenschaftlicher Forschung und beruflicher Praxis zusammengeführt und damit eine Brücke zwischen der Arbeit der UUX-Professionals und anderen Disziplinen, wie dem Security Engineering, geschlagen.

DANKSAGUNG

Die AutorInnen dieses Textes danken den übrigen Mitgliedern des Arbeitskreises Usable Security & Privacy. Teile dieser Arbeit sind im Rahmen des Forschungsprojektes „TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen“[4] sowie durch Forschung des Lehrstuhls Digitale Selbstbestimmung am Einstein Center for Digital Future [5] entstanden.

REFERENZEN

[1] Alizadeh, F., Jakobi, T., Boldt, J. and Stevens, G. 2019. GDPR-Reality Check on the Right to Access Data: Claiming and Investigating Personally Identifiable Data from Companies. Proceedings of Mensch Und Computer 2019 (New York, NY, USA, 2019), 811–814.

[2] Artikel-29-Gruppe Leitlinien für Transparenz gemäß der Verordnung 2016/679, angenommen am 29. November 2017 zuletzt überarbeitet und angenommen am 11. April 2018. Technical Report #WP 260 rev.01.

[3] Ausschuss für bürgerliche Freiheiten, Justiz und Inneres 2013. Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) -. Technical Report #A7-0402/2013. Europäisches Parlament.

[4] Balthasar, M., Gerl, A. Privacy in the toolbox of freedom, 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), Copenhagen, Denmark, 2019, pp. 1-4, doi: 10.1109/CMI48017.2019.8962146.

[5] Barth, S. and De Jong, M.D. 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and informatics. 34, 7 (2017), 1038–1058.

[6] Brunnbauer, Bernadette (2015) Visualisierung in der internationalen technischen Dokumentation. Masterarbeit, Universität Wien

[7] Bundesrat 2019. Entschließung des Bundesrates zum vorgesehenen Bericht der Europäischen Kommission über die Bewertung und Überprüfung gemäß Artikel 97 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Technical Report #570/199(B). Bundesrat.

[8] Cabinakova, J., Zimmermann, C. and Mueller, G. 2016. An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case. (2016).

[9] Elke Steven 2020. Verbesserung der DSGVO zum Schutz unserer Grundrechte: Empfehlungen der Digitalen Gesellschaft und des Verbraucherzentrale Bundesverbands (vzbv). Digitale Gesellschaft.

[10] Europäisches Parlament und der Rat 2018. Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[4] https://www.trusd-projekt.de/

[5] https://www.ziw.udk-berlin.de/forschung/digital-self-determination/

[11] Gerber, N., Reinheimer, B. and Volkamer, M. 2019. Investigating People's Privacy Risk Perception. Proceedings on Privacy Enhancing Technologies. 2019, 3 (2019), 267–288.
[12] Heimgärtner, R. (2012). Cultural Differences in Human-Computer Interaction. Towards Culturally Adaptive Human-Machine Interaction. Berlin, Boston: De Gruyter
[13] Jakobi, T., Patil, S., Randall, D., Stevens, G. and Wulf, V. 2019. It's About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering. ACM Trans. Comput.-Hum. Interact. 9, 4 (2019), 43. DOI:https://doi.org/10.1145/3281444.
[14] Joinson, A.N., Reips, U.-D., Buchanan, T. and Schofield, C.B.P. 2010. Privacy, trust, and self-disclosure online. Human–Computer Interaction. 25, 1 (2010), 1–24.
[15] Karwatzki, S., Trenz, M. and Veit, D. 2018. Yes, firms have my data but what does it matter? measuring privacy risks. (2018).
[16] Lepperhoff, N. and Müthlein, T. 2018. Leitfaden zur Datenschutz-Grundverordnung Umsetzungshilfe für die betriebliche Praxis, 2. Aufl.
[17] Marotta-Wurgler, F. 2019. Does "notice and choice" disclosure regulation work? An empirical study of privacy policies,".
[18] McDonald, A.M. and Cranor, L.F. 2008. The cost of reading privacy policies. Isjlp. 4, (2008), 543.
[19] Milne, G.R., Culnan, M.J. and Greene, H. 2006. A longitudinal assessment of online privacy notice readability. Journal of Public Policy & Marketing. 25, 2 (2006), 238–249.
[20] Nisbett, R.E., Peng, K., Choi, I. and Norenzayan, A. 2001. Culture and systems of thought: holistic versus analytic cognition. Psychological review. 108, 2 (2001), 291.
[21] Okasaki, D. Infographics in non western countries. Society for News Design (SND-E). Index Book. 66–81.
[22] Pettersson, J.S. 2014. A brief evaluation of icons suggested for use in standardised information policies: Referring to the Annex in the first reading of the European Parliament on COM (2012) 0011. Karlstads universitet.
[23] Polst, S., Kelbert, P. and Feth, D. 2019. Company Privacy Dashboards: Employee Needs and Requirements. International Conference on Human-Computer Interaction (2019), 429–440.
[24] Raschke, P., Küpper, A., Drozd, O. and Kirrane, S. 2017. Designing a GDPR-Compliant and Usable Privacy Dashboard. IFIP International Summer School on Privacy and Identity Management (2017), 221–236.
[25] Reidenberg, J.R., Breaux, T., Cranor, L.F., French, B., Grannis, A., Graves, J.T., Liu, F., McDonald, A.M., Norton, T.B., Ramanath, R., Russell, N.C., Sadeh, N. and Schaub, F. 2014. Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. Technical Report #ID 2418297. Social Science Research Network.
[26] Roy, H. 2014. Some comments on the EU's draft Privacy Icons: https://hroy.eu/posts/encryptionEuDataIcons/.
[27] Simon, H. A. 1955. A behavioral model of rational choice, Quarterly Journal of Economics, 69, 99–118
[28] Weber, W., Burmester, M. and Tille, R. 2013. Interaktive Infografiken. Springer-Verlag.
[29] Yoo, C.W., Ahn, H.J. and Rao, H.R. 2012. An exploration of the impact of information privacy invasion. (2012).

Autoren

Timo Jakobi ist wissenschaftlicher Mitarbeiter an der Professur Digitale Selbstbestimmung des Einstein Center for Digital Future und am Lehrstuhl für Wirtschaftsinformatik insb. IT-Sicherheit und Datenschutz an der Universität Siegen. Sein Forschungsschwerpunkt liegt auf der Entwicklung gebrauchstauglicher Unterstützungsmechanismen für das Management von Privatsphäre in IKT-Anwendungen. Hier stellt insbesondere der Trend zum Internet of Things mit der Anbindung und Analyse unterschiedlichster und abstrakter Daten(-quellen) eine neue Herausforderung dar, um Anwendern Transparenz und Kontrolle über die eigenen Daten zu verleihen.

Mandy Balthasar ist an der Universität der Bundeswehr München, wissenschaftliche Mitarbeiterin. Ihre Forschung, konzentriert sich auf das Verständnis und die Gestaltung von Mechanismen für kollektive Entscheidungsfindung und kollektives Verhalten, sowohl in künstlichen als auch in lebenden Kollektiven. Zuvor bewegte sie, als IT-Consultant, im Themenfeld der IT- und Informationssicherheit, Projekte im Management, der Mensch-Computer-Interaktion und dem Software-Engineering. Daraus ergibt sich ein besonderer Fokus ihres Engagements, auf die durch Menschenzentrierung geprägten Bereiche der Informatik: Sicherheit und Gesellschaft.

Martina Borkowsky ist User Experience Designerin beim Software-Unternehmen McAfee in den Niederlanden. Seit 2014 beschäftigt sie sich hier mit der Gestaltung der User Experience von Administratoren, die für den Datenschutz und die Datensicherheit in Unternehmen verantwortlich sind. Außerdem spricht sie als STEM Ambassador in Schulen und Universitäten und besucht Schüler, Lehrer, Eltern, Senioren zur Schulung im sicheren Umgang mit dem Internet und Security & Privacy.

Hartmut Schmitt ist Koordinator für Forschungsprojekte beim saarländischen IT-Lieferanten HK Business Solution GmbH. Er ist seit 2006 in Verbundvorhaben auf den Gebieten Mensch-Computer-Interaktion, Usability/User Experience und Software-Engineering tätig, u. a. als Projektkoordinator in mehreren BMBF- und BMWi-geförderten Verbundvorhaben.