von Grafenstein M. et al., Die Gestaltung wirksamer Bildsymbole für Verarbeitungszwecke und ihre Folgen für Betroffene Mithilfe einer interdisziplinären Forschungsmethodologie, In: Boden, A., Jakobi, T., Stevens, G., Bala, C. Hgg., Verbraucherdatenschutz – Technik und Regulation zur Unterstützung des Individuums. Schriften der Verbraucherinformatik Band 1, 2021. DOI: 10.18418/978-3-96043-095-7_07

Die Gestaltung wirksamer Bildsymbole für Verarbeitungszwecke und ihre Folgen für Betroffene Mithilfe einer interdisziplinären Forschungsmethodologie

RA Prof. Dr. Max von Grafenstein, LL.M.
Einstein Center Digital Future, Alexander von Humboldt Institut für Internet und Gesellschaft, Universität der Künste Berlin, Deutschland
m.von-grafenstein@udk-berlin.de

Julie Heumüller
Einstein Center Digital Future, Universität der Künste Berlin, Deutschland
j.heumueller@udk-berlin.de

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

Abstract. Unsere interdisziplinäre Forschungsarbeit „Die Gestaltung wirksamer Bildsymbole für Verarbeitungszwecke und ihre Folgen für Betroffene“ („Designing Effective Privacy Icons through an Interdisciplinary Research Methodology“) baut auf dem „Data Protection by Design“-Ansatz (Art. 25(1) DSGVO) auf und zielt auf folgende Forschungsfragen ab: Wie müssen das Transparenzprinzip (Art. 5(1)(a) DSGVO) und die Informationspflichten (Art. 12-14 DSGVO) insbesondere im Hinblick auf die Festlegung der Verarbeitungszwecke (Art. 5(1)(b) DSGVO) umgesetzt werden, damit sie die Nutzer:innen effektiv vor Risiken der Datenverarbeitung schützen? Mit welchen Methoden lässt sich die Wirksamkeit der Umsetzung ermitteln und diese auch durchsetzen?1 Im vorliegenden Projekt erweitern wir juristische Methoden um solche aus der HCI-Forschung (Human Computer Interaction) und der Visuellen Gestaltung. In einer ersten Phase haben wir mit empirischen Methoden der HCI-Forschung untersucht, welche Datennutzungstypen Nutzer:innen technologieübergreifend als relevant empfinden. Diese Erkenntnisse können als Ausgangspunkt für eine neue Zweckbestimmung dienen, die bestimmte Datennutzungstypen deutlicher ein- oder ausschließt. Erste Umformulierungen von Zweckbestimmungen haben wir in zwei Praxisworkshops mit Verantwortlichen der Datenverarbeitung getestet. In einer darauffolgenden qualitativen Studie untersuchten wir dann die Einstellungen und Erwartungen von Internetnutzerinnen und -nutzern am Beispiel der Personalisierung von Internetinhalten, um die entsprechenden Zwecke anhand eines konkreten Beispiels, in unserem Fall der personalisierten Werbung, neu zu formulieren. Auf dieser Basis haben wir nun die zweite Forschungsphase begonnen, in der wir Designs für Datenschutzhinweise und Kontrollmöglichkeiten unter besonderer Berücksichtigung des Verarbeitungszwecks entwickeln. Da der Einsatz von Cookies eine wichtige Rolle bei der Personalisierung von Werbung spielt, ist eine zentrale Aufgaben die Neugestaltung des sogenannten „Cookie-Banners“.

Das Zusammenspiel aus Icons, Text und Informations-/Kontrollarchitektur

Der vorliegende Beitrag fasst den aktuellen Zwischenstand unseres interdisziplinären Forschungsprojekts „Designing Effective Privacy Icons through an Interdisciplinary Research Methodology“ zusammen, das im August 2018 begonnen hat.

Das Projekt baut auf dem „Data Protection by Design“-Ansatz (Art. 25(1) DSGVO) auf und verfolgt die folgenden Forschungsfragen:

- Wie müssen, insbesondere bei der Angabe der Verarbeitungszwecke (Art. 5 Abs. (1)(b) DSGVO), der Transparenzgrundsatz (Art. 5 Abs. (1)(a) DSGVO) und die Informationspflichten (Art. 12-14 DSGVO) umgesetzt werden, damit sie die betroffenen Personen („data subjects“) wirksam vor Risiken der Datenverarbeitung schützen?

1 Siehe die Einreichung einer ersten Design-Studie und die damit gewonnenen vorläufigen Forschungsergebnisse im Wettbewerb der italienischen Datenschutzbehörde am 30. Mai 2021 (https://edpb.europa.eu/news/national-news/2021/easy-privacy-information-icons-yes-you-can-italian-dpa-launches-contest_en).

- Welche Rolle spielen Bildsymbole in diesem Zusammenhang?
- Welche Methoden können eingesetzt werden, um die Wirksamkeit der Umsetzung zu messen, sicherzustellen und durchzusetzen?

Die Zweckspezifizierung ist aus zwei Gründen der Ausgangspunkt unseres Projekts: Zum einen ist sie auch für die betroffenen Personen (die Nutzer:innen) der Ausgangspunkt, um die Verarbeitung ihrer personenbezogenen Daten angemessen beurteilen, die Nutzung dieser entsprechend einschränken und alle weiteren notwendigen Datenschutzmaßnahmen treffen zu können.
Zum anderen wird bei den derzeitigen Ansätzen, die sich mit Privacy Icons befassen, unseres Erachtens nicht ausreichend auf die Frage eingegangen, wie die Verarbeitungszwecke spezifiziert und durch Bildsymbole dargestellt werden müssen, damit die betroffenen Personen die Bedeutung der Datenverarbeitung tatsächlich verstehen.

Diese Forschungslücke geht auf einen blinden Fleck in der allgemeinen datenschutzrechtlichen Debatte über den Grundsatz der Zweckbindung zurück. Abgesehen von einer pauschalen Befürwortung oder Ablehnung des Zweckbindungsprinzips gibt es kaum vertiefte Ansätze, die sich mit der Frage auseinandersetzen, wie konkret die Zwecke zu benennen sind oder wie allgemein sie angegeben werden dürfen. Auch der Europäische Datenschutzausschuss (EDSA) beschränkt sich allein auf die Frage, welche Zweckbestimmungen zu allgemein sind, wenn keine genaueren Angaben gemacht werden (z. B. „Marketing“, „IT-Sicherheit“), ohne konkrete positive Vorschläge zu machen (Art. 29 Data Protection Working Party 2013). In früheren Arbeiten haben wir daher mithilfe juristischer Methoden Lösungsansätze entwickelt, mit denen die Frage, wie Verarbeitungszwecke angemessen spezifiziert werden können, zu beantworten ist (von Grafenstein 2020a; von Grafenstein 2020b; von Grafenstein 2021).

Im Gegensatz zu diesem juristisch-deduktiven Ansatz erweitern wir im vorliegenden Projekt unsere Methoden um solche aus der Human Computer Interaction (HCI)-Forschung und der Visuellen Gestaltung. In einer ersten Forschungsphase haben wir zunächst mit empirischen Methoden aus der HCI-Forschung sondiert, welche Datennutzungstypen betroffene Personen technologieübergreifend für relevant halten, um diese dann als Ausgangspunkt für eine verständlichere Zweckspezifizierung zu nutzen.
In zwei Praxisworkshops mit Teilnehmer:innen, die für die Datenverarbeitung verantwortlich sind (engl. „data controllers“), testeten wir diese ersten Neuformulierungen von Zweckspezifizierung. In der darauffolgenden qualitativen Studie untersuchten wir dann Einstellungen und Erwartungen von Internetnutzerinnen und -nutzern am Beispiel von personalisierten Internetinhalten, um die entsprechenden Zwecke anhand eines konkreten Beispiels (in unserem Fall anhand personalisierter Werbung) neu zu formulieren.

Die Ergebnisse dieser ersten Forschungsphase werden derzeit ausgewertet (von Grafenstein et al. in review).

Auf der eben geschilderten Grundlage haben wir nun unsere zweite Forschungsphase begonnen, in der wir Designs für Datenschutzhinweise und Kontrollmöglichkeiten mit speziellem Blick auf Verarbeitungszwecke entwerfen. Ob diese rein textlicher oder visueller Natur sind oder eine Kombination aus beidem beinhalten, ist dabei noch offen. Da die Verwendung von Cookies eine wichtige Rolle bei der Personalisierung von Werbung spielt, ist eine der zentralen Aufgaben hier die Neugestaltung des sogenannten „Cookie-Banners".

Der vorgelegte Beitrag ist ein erstes Zwischenergebnis unserer zweiten Forschungsphase. Neben den erklärenden Textpassagen zeigen die angehängten Abbildungen unseren ersten Prototypen einer Informationsarchitektur am Beispiel einer imaginären Website. Es handelt sich dabei wie erwähnt um erste Entwürfe – das Modell und insbesondere die integrierten Icons sind daher nicht endgültig.

Bisher sind die hier vorgestellten Entwürfe nur mit einzelnen Nutzer:innen getestet worden. Die vorgelegte Entwurfsskizze ist vielmehr als Ausgangspunkt für den nun folgenden partizipativen Gestaltungsprozess zu verstehen, in dem insbesondere betroffene Personen, aber auch Expert:innen sowie Datenverarbeiter:innen für die weitere Entwicklung der Entwürfe einbezogen werden sollen.

Wir hielten die Entwicklung einer ersten Designskizze noch vor der Beteiligung der oben genannten Akteure für notwendig, damit sich die Teilnehmer:innen des nun folgenden partizipativen Designprozesses konkrete Umsetzungsmöglichkeiten vorstellen können. Erste Versuche, die Nutzer:innen ohne visuelle Hilfestellungen (wie z. B. durch Skizzen) in den Gestaltungsprozess einzubeziehen, führten bei diesen in den meisten Fällen zu einer Überforderung, die konkrete Gestaltungsvorschläge blockierte.

Gleichzeitig hoffen wir, mit diesem Beitrag erste Forschungsergebnisse zum Diskurs über Privacy Icons beitragen zu können. Insbesondere möchten wir auf zwei aus unserer Sicht wichtige (wenn auch vorläufige) Forschungsergebnisse hinweisen:

1. Die Verarbeitungszwecke und ihre Folgen sollten für die betroffenen Personen als primäre Information durch Icons dargestellt werden.
2. Das Zusammenspiel aus Icons, Text und Informations- sowie Kontrollarchitektur ist als wesentliche Voraussetzung für die Wirksamkeit von Transparenz- und Kontrollmaßnahmen zu verstehen.

Die Grundstruktur: Unser dreistufiger Ansatz

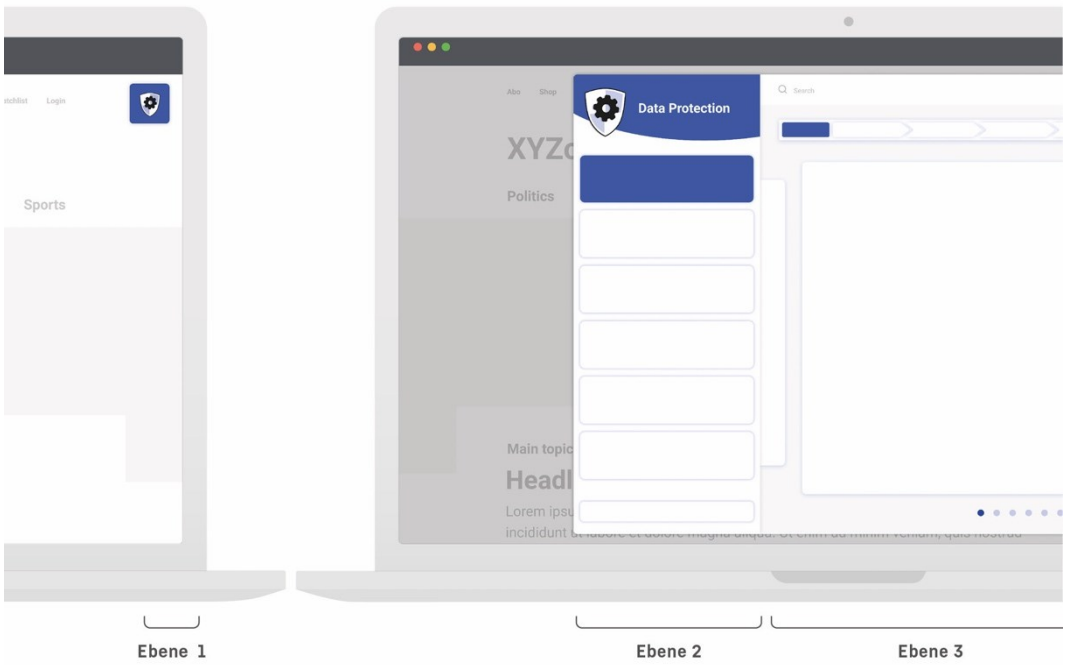

Abb. 1

Unser erster, vorläufiger Prototyp einer Informations- und Kontrollarchitektur ist über drei Ebenen aufgebaut. Die obenstehende Abbildung zeigt, wie sich unser Modell über die drei aufeinanderfolgenden Ebenen aufbaut:

- **Ebene 1:** Hierbei handelt es sich um unser Haupticon, das als sogenannter „Eye-Catcher“ in der oberen rechten Ecke der Webseite verortet ist und durchgehend, mithilfe eines Klicks der Nutzer:innen, als Einstiegspunkt unseres Modells dient.
- **Ebene 2:** Diese Ebene erreichen die Nutzer:innen vor allem über den Klick auf Ebene 1. Hier werden ihnen dann alle auf der besuchten Website vorhandenen Datenverarbeitungszwecke aufgelistet. Die Ebene 2 kann als einzelnes Fenster stehen oder wie in der Abb. 1 in Kombination mit der Ebene 3.
- **Ebene 3:** Auf dieser Ebene, die sich in Form eines größeren Fenster aufschiebt, erhalten die Nutzer:innen alle Informationen und Kontrollmöglichkeiten bezüglich ihrer personenbezogenen Daten. Diese beziehen sich immer auf den auf Ebene 2 ausgewählten Zweck.

Wird in den folgenden Seiten von „Ebene 1, 2 und 3“ gesprochen, nehmen wir auf die hier vorgestellten Ebenen Bezug.

Modifikation unserer Informationsarchitektur

Variante 1: Das Beispiel von Session-Cookies

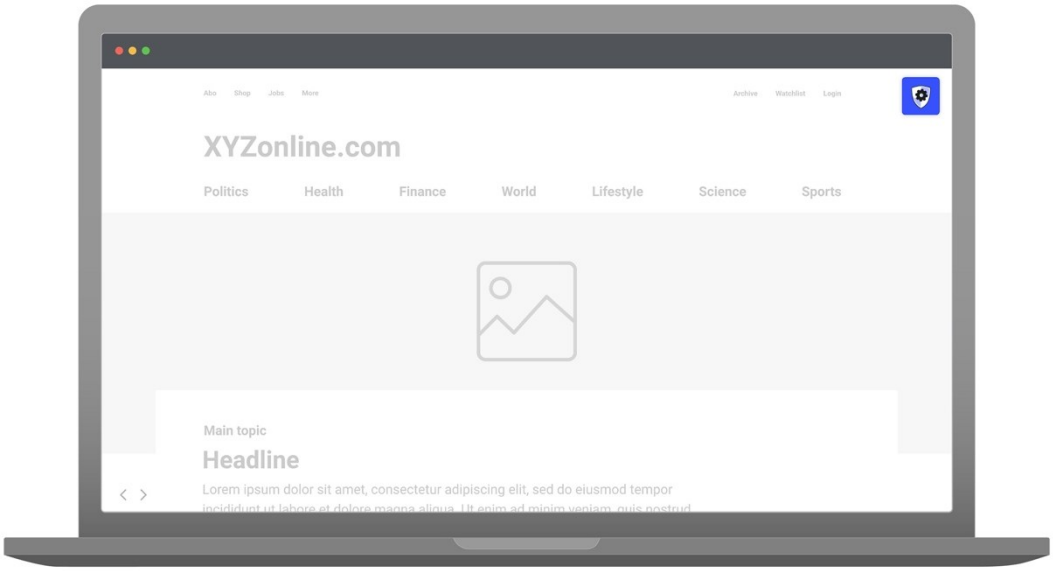

Abb. 2

Icons als Datenschutzsiegel

Unser Hauptsymbol bildet ein Siegel im Sinne des Art. 42 DSGVO. Die Idee dahinter ist, dass die Verwendung unserer Icons durch Zertifizierungsverfahren abgesichert wird, um einen möglichen Missbrauch (= Falschangabe) zu vermeiden und damit die Vertrauenswürdigkeit des Siegels langfristig zu gewährleisten. Das mit der Erteilung des Siegels verbundene Zertifizierungsverfahren stellt sicher, dass die zu zertifizierenden Verantwortlichen (d. h. deren Verarbeitungsvorgänge) auch die mit dem Icon verbundenen Datenschutzbestimmungen tatsächlich einhalten. Sind die Verarbeitungsverfahren einer Anwenderin oder eines Anwenders zertifiziert, darf das Icon mit seiner visuellen Signalwirkung von diesen auch für das eigene Marketing im Geschäftsverkehr verwendet werden.

In dem obigen Beispiel erscheint das Hauptsymbol unserer Informations- und Kontrollarchitektur in der oberen rechten Ecke einer Website. Es besteht aus einem Schutzschild mit einem Zahnrad in der Mitte, das eine doppelte Bedeutung besitzt: Sinnbildlich steht dieses sowohl für den Begriff „Datenverarbeitung“ als auch für „Einstellungen“. Damit werden die beiden Kernelemente des Datenschutzes in einem Symbol zusammengefasst und in den Mittelpunkt gestellt:

einerseits die Möglichkeit für die betroffenen Personen, in die Verarbeitung ihrer personenbezogenen Daten einzugreifen, andererseits symbolisiert das Schutzschild unter dem Zahnrad die durch das Zertifizierungsverfahren gewährleisteten Datenschutzmaßnahmen.

An allen Stellen im Modell, an denen es möglich ist, bevorzugen wir die Kombination aus Icons und einer kurzen Beschriftung. Hiermit wird die Verständlichkeit der überlieferten Information maximiert. Eine Ausnahme bildet unter anderem unser Haupt-Icon auf der in Abb. 2 gezeigten Ebene 1. Da es in seiner Signalfunktion auf (zertifizierten) Webseiten immer als anklickbare Schaltfläche in der oberen rechten Ecke sichtbar ist, haben wir uns hier gegen eine zusätzliche Beschriftung entschieden.

Für den Fall der Farbenblindheit bei Nutzer:innen sind unsere Icons doppelt kodiert: durch Farbe und Form.

Nach unseren bisherigen Erkenntnissen hängt die Wirksamkeit der Gestaltung und Platzierung von Datenschutz-Icons vom Nutzungskontext der Nutzer:innen ab, in dem ihnen bestimmte Informationen präsentiert werden. Wie bereits erwähnt, haben wir uns für einen Mehr-Ebenen-Ansatz bei der Darstellung von Datenschutzhinweisen und damit auch hinsichtlich der Gestaltung und Platzierung unserer Datenschutzsymbole entschieden.

Das Beispiel von Cookie-Banners

Ein erstes Beispiel für unseren mehrstufigen Ansatz sind die Datenschutzhinweise zum Setzen von Cookies im jeweiligen Browser des Endgeräts. In unserem Beitrag wird zwischen drei Arten von Cookies unterschieden, auf die je nach Verwendungszweck (und den damit verbundenen verschiedenen Konsequenzen für die Betroffenen) unserer Ansicht nach unterschiedlich hingewiesen werden muss. Diese Unterschiede haben in unseren Designentwürfen sowohl eine Auswirkung auf die Informationsarchitektur als auch auf die Wahl der Icons.

In dem in Abb. 2 gezeigten ersten Anwendungsfall verwendet die Website nur Session-Cookies (z. B., um die Informationen in einem Online-Formular während der gesamten Sitzung zu erhalten). Unserer Rechtsauffassung nach sollten in diesem Fall die Nutzer:innen kein Wahlrecht haben, diesen Session-Cookies zuzustimmen oder ihnen zu widersprechen, da sie nur minimal invasive Folgen für Nutzer:innen haben, für die Funktionalität der Website jedoch notwendig sind. Ein sogenannter „Cookie-Banner" ist daher nicht erforderlich. Den Nutzer:innen wird auf dieser Website als Einstiegspunkt in unsere Informationsarchitektur also nur das Hauptsymbol angezeigt, über das sie durch Anklicken zu den Ebenen 2 und 3 gelangen können.

Auf der Ebene 2 werden den Nutzer:innen dann alle Verarbeitungszwecke aufgelistet, die auf der besuchten Website Anwendung finden. Dazu gehört der

primäre Zweck der Darstellung der Webseite (»Service«), für den das Session-Cookie erforderlich ist. Wegen den erwähnten schwachen Folgen des Session-Cookies für die Nutzer:innen wird dieses Cookie selbst erst auf unserer Ebene 3 erwähnt (im Zusammenhang mit der Frage, wie Nutzer:innen der Website technisch identifiziert werden, d. h. welche Identität sie in den Augen des Website-Betreibenden haben).

Variante 2: Das Beispiel von funktionalen Cookies

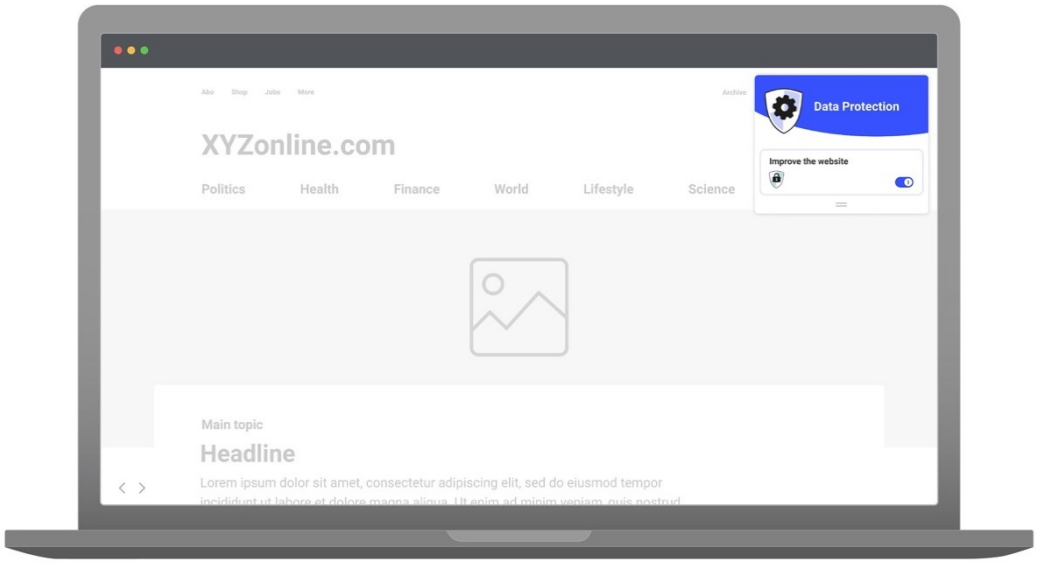

Abb. 3

Die Bedeutung von Informations- und Kontrollarchitekturen

In dem hier gezeigten zweiten Anwendungsfall verwendet der Website-Betreiber nicht nur Session-Cookies, sondern auch funktionale Cookies. Da die Verarbeitungszwecke von diesen schwerwiegendere Folgen für die Nutzer:innen der Website haben als Session-Cookies, wirkt sich dies auch auf unsere Informationsarchitektur aus. Folglich ist der Aufbau und damit der Einstiegspunkt unseres Modells beim Aufrufen einer solchen Website ein anderer als der zuvor geschilderte erste Fall.

Nach Aufrufen der Webseite klappt sich das Hauptsymbol (Ebene 1) nach links unten aus (Ebene 2) und bietet den Nutzer:innen der Seite die wichtigsten Informationen und Kontrollmöglichkeiten. Die textliche Klarstellung, dass es sich bei dem Haupticon um einen Datenschutzhinweis handelt, erscheint nun auch in der Kopfzeile.

Funktionale Cookies werden beispielsweise verwendet, um nach unserem hier vertretenen Verständnis die Reichweite der Website zu messen. Da diese Cookies für das Ausspielen der Webseite (d. h. die eigentliche „Dienstleistung“) nicht zwingend notwendig sind, aber außer einem Eingriff durch das Setzen des Cookies und den dadurch ermöglichten rudimentären Einblicken in die Privatsphäre der Nutzer:innen keine weiteren Folgen für jene nach sich ziehen, sollten Nutzer:innen hier kein Recht auf Zustimmung, sondern nur ein Widerspruchsrecht haben. Der Kippschalter ist daher in diesem Beispiel auf „An“ gesetzt.

Unserer Meinung nach ist es weniger wichtig, den Nutzer:innen das Setzen von Cookies zu erklären, als vielmehr den Zweck der durch sie gesammelten Daten. Aus diesem Grund wird der (unseres Erachtens wenig aussagekräftige) Hinweis auf das Cookie nicht auf Ebene 2 angezeigt. Stattdessen wird explizit auf den Zweck der mit dem Cookie verfolgten Datenverarbeitung und auf die Auswirkung auf die Privatsphäre der Nutzer:innen hingewiesen.

Privacy Icons als Hinweis auf Konsequenzen

Der technische Zweck wird durch die Überschrift „Verbesserung des Dienstes“ („Improve the website“) dargestellt. Auf die Folgen oder möglichen Folgen dieses Datenverarbeitungszwecks wird visuell mittels eines Privacy-Icons hingewiesen. Dieses Icon zeigt das oben bereits erwähnte Siegel in Kombination mit einem Schloss; dieses soll das Konzept der Achtung der Privatsphäre widerspiegeln, demzufolge andere Personen von der eigenen Privatsphäre ausgeschlossen werden können (d. h. ihnen der Zugang zu dieser gestattet oder verweigert werden kann).

Wie zuvor bei den Session-Cookies wird auch hier das Setzen des Cookies selbst erst auf Ebene 3 explizit erklärt (im Zusammenhang mit der technischen Identifizierung der Nutzer:innen der Website). Indem Nutzer:innen auf das Feld „Verbesserung des Dienstes“ klicken, können sie auf diese Ebene zugreifen und die Informationen erhalten.

Durch ein Mouse-Over über den Doppelbalken am unteren Ende der Ebene 2 werden den Nutzer:innen alle weiteren Zwecke angezeigt, für die personenbezogene Daten auf der Website erhoben werden – für welche die Nutzer:innen aber keine unmittelbare Kontrollmöglichkeit besitzen (d. h., es gibt hier keinen Kippschalter für die Einwilligung oder Ablehnung dieser Zwecke). So berücksichtigt unser Modell aufmerksamkeitsökonomische Erwägungen, indem es die Aufmerksamkeit der Nutzer:innen auf die Zwecke lenkt, bei denen sie direkt eingreifen können. Natürlich besteht jederzeit die Möglichkeit, bei ausgeklappter Ebene 2 auf alle aufgelisteten Zwecke zu klicken und damit auf die dritte Ebene zu gelangen, auf der Nutzer:innen weitgehende Informationen zu allen Zwecken erhalten.

In dem hier besprochenen zweiten Anwendungsfall schließt sich die Ebene 2 (also das »Cookie-Banner«) automatisch, wenn die Nutzer:innen keines der Felder unserer Informationsarchitektur anklicken, sondern mit der Webseite selbst interagieren (also durch Scrollen oder Klicken).

Aufgrund der geringen Auswirkung funktionaler Cookies ist nach unserer derzeitigen Auffassung dem Schutzbedürfnis der Nutzer:innen somit Genüge getan, wenn dieser Hinweis automatisch beim Aufrufen der Webseite erscheint, aber auch wieder automatisch verschwindet, wenn die Nutzer:innen beginnen, mit der Website zu interagieren. Möchten die Nutzer:innen zu einem späteren Zeitpunkt der Datenverarbeitung widersprechen, können sie jederzeit auf die Ebene 2 zugreifen, indem sie auf das Hauptsymbol in der oberen rechten Ecke klicken, das dort immer fixiert bleibt.

Empirische Tests zur Anpassung der Informations- und Kontrollarchitekturen

Mit diesem Beispiel möchten wir zeigen, dass die Informations- und Kontrollarchitektur für eine effektive Umsetzung von Transparenz- und Kontrollmöglichkeiten mindestens genauso wichtig ist wie die Gestaltung und Platzierung der Privacy Icons selbst. Bei der konkreten Ausgestaltung der Informations- und Kontrollarchitektur gibt es zudem deutlich mehr Spielraum, als die unseres Erachtens sehr oberflächlich geführte Debatte um das „Opt-In-“ oder „Opt-Out-Verfahren“ vermuten ließe. Auch ist nicht jede bewusst gesetzte Informations- und Kontrollarchitektur ein sogenanntes „Dark Pattern“ (Norwegian Consumer Council 2018). Selbstverständlich ist mit juristisch-empirischen Methoden näher zu untersuchen, inwieweit einzelne Informations- und Kontrollarchitekturen angesichts bekannter Entscheidungsheuristiken und der jeweiligen Datenschutzrisiken die Entscheidungsmöglichkeiten der Nutzer:innen zulässigerweise wahren oder unzulässig einschränken (Grafenstein et al. 2018). Auch gehen wir davon aus, dass unsere hier dargestellte Informations- und Entscheidungsarchitektur aufgrund weiterer empirischer Tests angepasst werden wird.

Variante 3: Das Beispiel von Marketing-Cookies (für personalisierte Werbung)

Zusätzliche Informations- und Kontrollmechanismen sind mindestens so wichtig wie die Zustimmung selbst

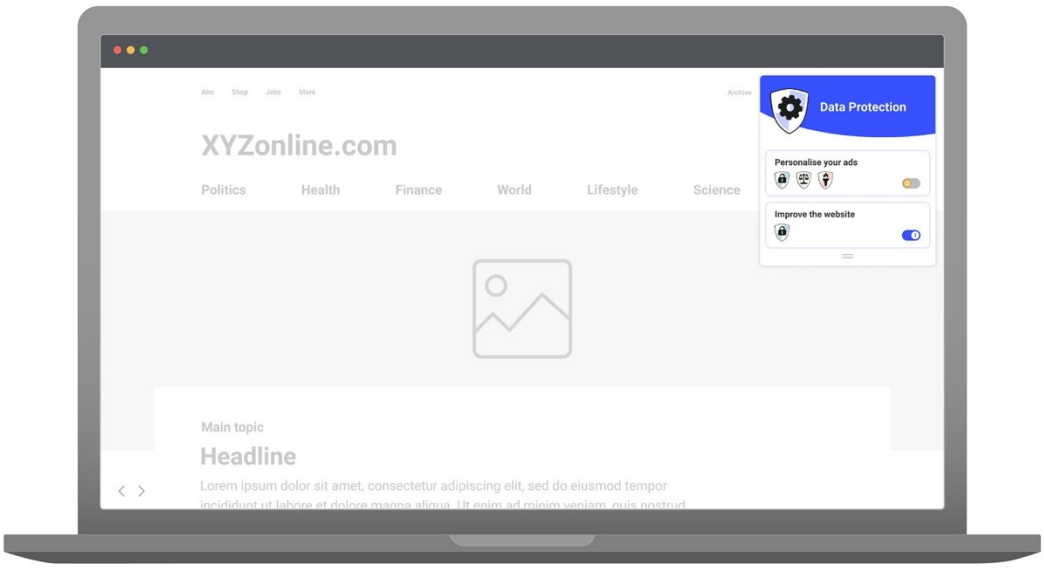

Abb. 4

Nutzer:innen zu den „Ownern“ ihrer Profile machen

Im dritten Anwendungsfall werden Cookies zum Zweck der personalisierten Werbung gesetzt. Diese Marketing-Cookies haben schwerwiegendere Folgen für die betroffenen Personen als die zuvor angesprochenen Session- und funktionalen Cookies. Daher wird die Information über diesen Zweck nicht nur automatisch beim Aufruf der Website angezeigt, sondern direkt an erster Stelle auf der Ebene 2.

Allerdings halten wir auch hier (d. h. bei Marketing-Cookies) die Information über die Folgen für die Nutzer:innen für wichtiger als das Setzen der Cookies an sich. Das Setzen der Cookies wird daher wie schon bei den anderen Beispielen erst auf Ebene 3 angezeigt.

Im Gegensatz zu den anderen bereits erwähnten Zwecken hat der Zweck der personalisierten Werbung jedoch nicht nur durch das Profiling von Nutzer:innen größere Auswirkungen auf deren Privatsphäre, sondern stellt auch eine Bedrohung für ihre Entscheidungs- und Diskriminierungsfreiheit dar. Erstere liegt dabei in der möglichen Manipulation der Kaufentscheidung der Nutzer:innen, indem ihnen speziell auf sie zugeschnittene – also personalisierte – Werbung angezeigt wird. Eine Gefahr der Diskriminierung besteht in der schlichten Tatsache, dass ihnen

unterschiedliche Werbungen angezeigt werden und sie somit unterschiedlich behandelt werden.

Diese mehr oder weniger gravierenden zusätzlichen Risiken werden durch zwei weitere Privacy-Icons dargestellt. Im Fall einer Diskriminierungsgefahr zeigen sie das Siegel in Kombination mit einer Waage und im Falle einer Gefahr der Entscheidungsfreiheit das Siegel mit einer Freiheitsfackel.

In unseren aktuellen Skizzen werden diese Risiken auf Ebene 2 nicht weiter spezifiziert. Obwohl z. B. das Profiling viel mehr Einblicke in das Privatleben der Nutzer:innen gewährt als Session- und funktionale Cookies, spiegelt das Privacy-Icon mit dem Schloss diese Unterschiede auf der Ebene 2 noch nicht wider. Hinter dieser Designentscheidung steht der Gedanke, dass wir die Anzahl der auf Ebene 2 verwendeten Icons gering halten möchten, um die Nutzer:innen nicht mit zu vielen verschiedenen Symbolen auf dieser zweiten Ebene zu überfordern. Aktuell werden erst auf Ebene 3 mehr Icons eingeführt, um die Unterschiede zwischen den Eingriffen der Verarbeitungszwecke zu verdeutlichen.

Wegen des schwerwiegenderen Eingriffs in die Grundrechte der Nutzer:innen sollte der Zweck der personalisierten Werbung auch nach unserer bisherigen Meinung nur auf deren vorheriger Zustimmung beruhen. Der Kippschalter ist daher standardmäßig auf „Aus" gesetzt. Zu beachten ist allerdings, dass unser Schutzsystem es den betroffenen Personen weitestgehend ermöglicht, die tatsächlichen Risiken dieses Zwecks im Detail zu kontrollieren. Zum Beispiel wird das Manipulationsrisiko dadurch minimiert, dass in jeder personalisierten Bannerwerbung den Nutzer:innen unser Hauptsymbol in verkleinert Form angezeigt wird. Ihnen wird damit zum einen die Personalisierung der Werbung kenntlich gemacht und zum anderen können sie durch einen Klick auf dieses Symbol direkt zu ihrem Profil auf Ebene 3 gelangen, auf dessen Grundlage die Werbung für sie personalisiert wird (siehe auch Einstiegspunkt 3). Auf diese Weise können sie nach unserem Gestaltungsanspruch die Personalisierung der Werbung in ihrem konkreten Nutzungskontext verstehen und kontrollieren; so behalten sie ihre Autonomie bei möglichen Kaufentscheidungen (siehe hierfür auch „Variante 3 – Extension, S. 16").

Das Risiko der Diskriminierung kann ebenfalls vermieden werden, indem die Nutzer:innen jederzeit die Möglichkeit haben, die Personalisierung wieder abzuschalten. Hierfür ziehen sie einfach ihre Zustimmung zurück, indem sie auf Ebene 2 den Kippschalter auf „Aus" setzen. Auf diese Weise erhalten sie nicht nur auf der Webseite einen unmittelbaren visuellen Vergleich personalisierter und nicht personalisierter Werbung, sondern können im selben Nutzungskontext die ihnen zugeordneten Interessen sowie die zugrunde liegenden Rohdaten einsehen, anpassen und löschen/sperren.

Unser Schutzsystem soll so die Nutzer:innen zu „Ownern“ ihres Profils machen, indem sie nicht nur die Risiken so weit wie möglich kontrollieren, sondern auch die Personalisierung an ihre tatsächlichen Bedürfnisse anpassen können.

Aufgrund des so erreichten Schutzniveaus halten wir es in der vorliegenden Skizze für testwürdig, die drei folgenden „Nudges“ zu setzen, um zumindest die Wahrscheinlichkeit zu erhöhen, dass die Nutzer:innen diese Optionen tatsächlich in Betracht ziehen.

Abb. 5

Abb. 6

Erster Nudge: Wenn die Nutzer:innen auf die Website klicken oder nach unten scrollen, verschwindet auf Ebene 2 automatisch der Hinweis auf den Zweck „Verbesserung des Dienstes“ („Improve the website“). Der Hinweis auf personalisierte Werbung hingegen („Personalise your ads“) verschwindet erst, wenn die Nutzer:innen auf das dafür vorgesehene Kreuz („x“) in der linken oberen Ecke des Banners klicken (siehe Abb. 5).

Zweiter Nudge: Wenn die Nutzer:innen ihren Mauszeiger über das weiße Feld „Personalise your ads“ bewegen, erscheint eine Meldung mit etwa folgender Information: „Sie sind genervt von Cookie-Bannern? Klicken Sie hier und nehmen Sie Ihrer Einstellungen einmal vor – für immer” („You’re annoyed from cookie banners? Click here and control once.“, siehe Abb. 6).

Die hier von den Nutzer:innen vorgenommen Einstellungen werden gespeichert (über ein separates Cookie oder ein Login – entsprechende Informationen werden den Nutzer:innen dazu auf Ebene 3 gegeben), sodass das Banner in zukünftigen Sitzungen nicht mehr angezeigt wird. Allerdings gelangen die Nutzer:innen bei zukünftigen Besuchen von Websites durch Anklicken des Hauptsymbols in der oberen rechten Ecke der Website immer zu den Ebenen 2 und 3, wo sie ihre Einstellungen jederzeit ändern können.

Dritter Nudge: Durch das Anklicken des in Abb. 6 gezeigten blauen Feldes geben die Nutzer:innen automatisch ihr Einverständnis. Durch diesen Klick gelangen sie zu Ebene 3 mit den Informations- und Kontrollmöglichkeiten und der Kippschalter stellt sich automatisch auf „An“.

Um sicherzustellen, dass diese drei aufgezählten Nudges kein sogenanntes „Dark Pattern“ bilden, dürfen sie das Verhalten der Nutzer:innen nicht unangemessen zugunsten der Einwilligung oder zum Nachteil des Wegklickens des Banners beeinflussen. Positiv gewendet sind diese Nudges nur dann „Good Nudges“, wenn sie die betroffenen Personen tatsächlich in die Lage versetzen, eine informierte autonome Entscheidung für oder gegen die Verarbeitung ihrer personenbezogenen Daten zu einem bestimmten Zweck zu treffen – trotz verhaltensbedingter Biases (Grafenstein et al. 2018).

Voraussetzung für die Vermeidung eines „Dark Pattern“ ist in diesem Fall, dass das Kreuz zum Schließen des Bereichs („x“) ebenso gut wahrnehmbar und leicht zu bedienen ist wie der Einwilligungsknopf (in Form des Kippschalters). Umgekehrt handelt es sich um „Good Nudges“, wenn die hier vorgestellte Informationsarchitektur den sogenannten „By Default Bias“ des klassischen Einwilligungsprozesses überwindet, wonach Nutzer:innen oftmals schlicht nur deshalb nicht einwilligen, weil sie es aktiv tun müssen. Unserer Meinung nach

kann die vorliegende Architektur diese Verzerrung teilweise kompensieren. Die Gültigkeit unserer Einschätzung bedarf freilich empirischer Verifikation.

Variante 3 – Extension:
Das Beispiel der personalisierten Werbung

Abb. 7

Kenntlichmachung des Risikos

Wie bereits erwähnt, zielt unser Schutzsystem darauf ab, über unmittelbar im jeweiligen Wahrnehmungskontext verfügbare Information zu den Gründen der angezeigten Werbung das Risiko der Manipulation zu minimieren. Dafür sehen wir in unserem Design-Konzept vor, dass in einer Ecke eines personalisierten Werbebanners unser Hauptsymbol erneut angezeigt wird – ein Symbol also, das die Nutzer:innen bereits mit ihren Datenschutzeinstellungen in Verbindung bringen. Wenn sie auf dieses Symbol klicken, werden sie direkt zu ihrem Interessenprofil auf Ebene 3 weitergeleitet, auf dessen Grundlage die Werbung für sie personalisiert wird. Auf diese Weise können die Nutzer:innen die Personalisierung der Werbung innerhalb ihres konkreten Nutzungskontext nachvollziehen, sie kontrollieren und damit – zumindest nach unserer Vorstellung – ihre Autonomie bei Kaufentscheidungen behalten.

Ebene 3: Unser Privacy Dashboard

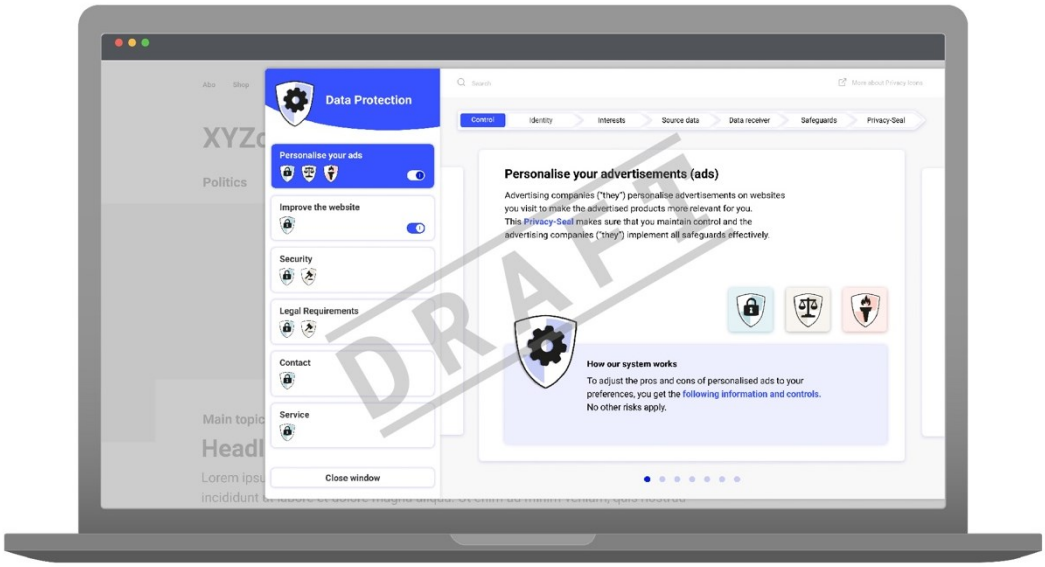

Abb. 8

In diesem Abschnitt möchten wir noch einen Blick auf die Ebene 3 unserer Design-Skizze werfen, die wir als „Privacy Dashboard“ verstehen, weil auf ihr den Nutzerinnen und Nutzern detaillierte Informationen und Kontrollwerkzeuge angeboten werden. Hier können die Nutzer:innen demnach alle Informationen gemäß Artikel 13 und 14 der DSGVO erhalten und ihre Rechte als betroffene Person gemäß Artikel 15 bis 21 der DSGVO ausüben. Die Wirksamkeit der Umsetzung der vorgenannten Bestimmungen der DSGVO beruht konzeptionell auf der Tatsache, dass die Informationen und die Rechte der betroffenen Personen im spezifischen Nutzungskontext zur Verfügung gestellt werden. Die betroffenen Personen erhalten also die Informationen und Eingriffsrechte dann, wenn sie aus Sicht der Nutzer:innen am kontextuell relevantesten sind. Gleichzeitig sind die Informations- und Kontrollarchitekturen auf den Ebenen 1 bis 3 so gestaltet, dass sie so wenig wie möglich in das eigentliche Bestreben der Nutzer:innen, nämlich den Besuch der Website, eingreifen.

Das „Privacy Dashboard“ besteht zum einen links aus der Ebene 2, die nach wie vor alle Verarbeitungszwecke der Website auflistet und zum anderen, rechts daran angeschlossen, aus einem größeren Fenster, auf dem den Nutzer:innen zweckspezifische Informationen und Interventionsmöglichkeiten abgebildet werden (oben in Abb. 8 auf der linken Seite als blaues Feld zu sehen).

Der Fortschrittsbalken im oberen Bereich dieses Fensters dient sowohl als Navigationsleiste als auch als Steuerelement. Er zeigt an, unter welchem Unterpunkt sich die Nutzer:innen gerade beim ausgewählten Zweck befinden.

Insgesamt gibt es am Beispiel des Zwecks „Personalisierte Werbung“ sieben solcher Unterpunkte, die die Nutzer:innen Schritt für Schritt durch die Informationen und Kontrollmöglichkeiten leiten.

Der erste Unterpunkt „Kontrolle“ (in Abb. 8 „Control“) erläutert insbesondere die Bedeutung der bereits auf Ebene 2 verwendeten Icons. Hier kommen weitere konkretisierende Icons ins Spiel. Klicken die Nutzer:innen beispielsweise auf die grün eingefärbte Kachel mit dem Schloss-Icon (wie oben erklärt: symbolisch für die Privatsphäre der Nutzer:innen), geht die Informationsbox eine Ebene tiefer und erläutert nun, inwieweit der jeweilige Zweck die Privatsphäre der Nutzer:innen beeinträchtigt (hier: durch Profiling).

Wesentlich für das vorgestellte Schutzsystem ist die Rechtstatsache, dass alle dargestellten Risiken, die durch die Informations- und Kontrollmöglichkeiten kontrolliert werden, Teil der Zweckerklärung sind (siehe Verweise in der Einleitung oben). Dies bedeutet, dass die nachfolgende Verarbeitung keine weiteren Risiken verursachen darf. Entstehen durch eine Zweckänderung neue Risiken, muss ihre datenschutzrechtliche Zulässigkeit bzw. die zugrunde liegende Zweckänderung auf ihre Zweckkomptabilität gemäß Art. 6 (4) DS-GVO geprüft werden. Daher stellen wir unter dem ersten Unterpunkt „Kontrolle“ auch direkt im letzten Satz der Info-Box klar, dass mit diesem Zweck weitere spezifische Risiken ausgeschlossen sind.

Die weiteren Unterpunkte des Fortschrittsbalken, insbesondere „Identität“ bis „Schutzmaßnahmen“ (in Abb. 8 „Identity“ bis „Safeguards“) zeigen schließlich im Detail auf, welche Einblicke in das Privatleben der Nutzer:innen konkret durch das Profil generiert werden und wie die Nutzer:innen diese sowie die sonstigen Risiken kontrollieren können.

Fazit: Der Stand der Technik von Transparenz- und Kontrollmaßnahmen (sowie seine Durchsetzung durch Datenschutzbehörden)

Artikel 25 (1) der DSGVO verpflichtet die für die Datenverarbeitung Verantwortlichen, die Grundsätze der Zweckbindung und der Transparenz sowie die Informationspflichten und die Rechte der betroffenen Person durch technische/organisatorische Maßnahmen umzusetzen, um deren Grundrechte wirksam gegen die Risiken der Verarbeitung ihrer personenbezogenen Daten zu schützen.

Der Begriff „wirksam" bedeutet dabei, die tatsächlichen Auswirkungen der Schutzmaßnahmen in die rechtliche Bewertung einzubeziehen, was empirische Methoden zur Überprüfung der Wirksamkeit erfordert (Art. 29 Data Protection Working Party 2017; EDPB 2020 cip. 7).

So wird beispielsweise mit mathematisch-statistischen Methoden ermittelt, ob Anonymisierungs- oder Verschlüsselungsverfahren den Grundsatz der Datenminimierung oder der Vertraulichkeit so umsetzen, dass sie zu einem wirksamen Schutz der Privatsphäre der Betroffenen führen. Hängt dagegen die Wirksamkeit von Schutzmaßnahmen von ihrer Verständlichkeit und Nutzbarkeit bei den Nutzer:innen ab, wie dies bei Transparenz und Kontrolle der Fall ist, kann sie nicht mit den eben genannten Methoden nachgewiesen werden. Hier werden stattdessen Methoden aus der UX- oder Human Computer Interaction (HCI)-Forschung benötigt. Darüber hinaus können diese UX- oder HCI-Methoden der Feststellung dienen, ob bestimmte Icons, Texte und/oder Informations- und Kontrollarchitekturen die Nutzer:innen besser vor Datenschutzrisiken schützen als andere Umsetzungsoptionen. Dies wiederum ist entscheidend für die Anforderung an den Stand der Technik (von Grafenstein et al. in review).

Denn nach Artikel 25 der DSGVO müssen die für die Datenverarbeitung Verantwortlichen nicht nur die Schutzmaßnahmen wirksam umsetzen, sondern auch den Stand der Technik („state of the art") berücksichtigen. Unter diesem ist die wirksamste auf dem Markt verfügbare Technologie zu verstehen (vgl. Martini 2000; Baumgartner and Gausling 2017; Grafenstein 2019).

Mit anderen Worten: Wenn sich ein Icon, ein Text oder eine Informations- und Kontrollarchitektur als die effektivste Maßnahme erweist, stellt sie den aktuellen für den jeweiligen Verarbeitungszweck (und die mit ihm verbundenen Risiken) geltenden Stand der Technik dar – bis sich eine noch effektivere Umsetzung der DSGVO-Vorschriften im fortlaufenden Forschungs- und Entwicklungsprozess herausbildet.

Auf dieser methodologischen Grundlage könnten sinnlose Cookie-Banner bald der Vergangenheit angehören. Voraussetzung dafür ist allerdings, dass die

zuständigen Datenschutzbehörden die dafür entwickelten Konzepte und Methoden anwenden und den Stand der Technik in der Praxis durchsetzen.

Anmerkung:

Der hier eingereichte Beitrag beruht auf unserem bereits im Mai 2021 eingereichten Dokument „Designing effective icons for processing purposes and its consequences through an interdisciplinary research methodology“, das wir im Rahmen des Wettbewerbs „Easy privacy information via icons? Yes, you can!“ bei der italienischen Datenschutzbehörde eingereicht haben.

Wir möchten uns an dieser Stelle außerdem bei unserem gesamtem Forschungsteam „Digitale Selbstbestimmung“ bedanken.

Literatur

Art. 29 Data Protection Working Party (2013) Opinion 03/2013 on purpose limitation

Art. 29 Data Protection Working Party (2017) Guidelines on transparency under Regulation 2016/679

Baumgartner U, Gausling T (2017) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. ZD (07):308–313

EDPB (2020) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0, adopted on 20 October 2020

Grafenstein M (2019) Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design. In: González-Fuster G, van Brakel R, De Hert P (eds) Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, Edward Elgar Publishing. Edward Elgar Publishing

Grafenstein M von, Hölzel J, Irgmaier F, Pohle J (2018) Nudging: Regulierung durch Big Data und Verhaltenswissenschaften. Abida – Assessing Big Data

Martini M (2000) Integrierte Regelungsansätze im Immissionsschutzrecht: eine Untersuchung zu dem integrierten Ansatz der UVP-RL, der IVU-RL und der Öko-Audit-Verordnung sowie ihrer deutschen Umsetzungsgesetze, 1. C. H. Beck

Norwegian Consumer Council (2018) Deceived by design - How tech companies use dark patterns to discourage us from exercising our rights to privacy. Norwegian Consumer Council

von Grafenstein M (2020a) Refining the Concept of the Right to Data Protection in Article 8 ECFR - Part I: European Data Protection Law Review. EDPL

von Grafenstein M (2020b) Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II: Controlling Risks through (Not To) Article 8 ECFR against the Other Fundamental Rights (Esp. by the Principle of Purpose Limitation). Social Science Research Network, Rochester, NY

von Grafenstein M (2021) Refining the Concept of the Right to Data Protection in Artile 8 ECFR - Part III: Consequences for the interpretation of the GDPR (and the lawmaker's room for maneuver). EDPL

von Grafenstein M, Jakobi T, Stevens G (in review) Effective Data Protection by Design through interdisciplinary research methods - The example of effective purpose specification by applying user-centered UX-design methods. CLSR