

7. September 2020

Innovatives Datenschutz- Einwilligungsmanagement

Abschlussbericht

vorgelegt bei:

Bundesministerium der Justiz und für
Verbraucherschutz
Mohrenstraße 37
10117 Berlin

durch:

ConPolicy GmbH
Institut für Verbraucherpolitik
Crellestr. 37
10827 Berlin
www.conpolicy.de

Autoren:

Dr. Sara Elisa Kettner
Prof. Dr. Christian Thorun
Prof. Dr. Gerald Spindler

gemeinsam mit:

Prof. Dr. Gerald Spindler
Lehrstuhl für Bürgerliches Recht, Handels- und Wirt-
schaftsrecht, Multimedia- und Telekommunikations-
recht, Rechtsvergleichung
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 6
37073 Göttingen

Zusammenfassung

Die datenschutzrechtliche Einwilligung stellt ein wesentliches Instrument für den Schutz der Privatsphäre dar. Gemäß den Vorgaben der Datenschutz-Grundverordnung muss eine Einwilligung informiert, differenziert und freiwillig erfolgen. Um diese Anforderungen sowohl rechtssicher als auch nutzerfreundlich umzusetzen, sind Einwilligungsmanagement-Systeme (EMS) nötig.

Vor diesem Hintergrund hat das Bundesministerium der Justiz und für Verbraucherschutz das Forschungsvorhaben „Innovatives Datenschutz-Einwilligungsmanagement“ beauftragt. Hier wurden bereits vorhandene Modelle von EMS im Online-Kontext analysiert, Verbrauchererwartungen an solche empirisch im Rahmen einer repräsentativen Online-Befragung mit 2.029 Personen sowie zwei Praxistests bei Miele und der Telekom erhoben und im Ergebnis Handlungsempfehlungen zur rechtskonformen und nutzerfreundlichen Einwilligung in Form eines Best Practice-Modells entwickelt.

Das zentrale Ergebnis der Studie ist, dass es Möglichkeiten gibt, die **Vorgaben der Datenschutz-Grundverordnung sowohl rechtskonform als auch nutzerfreundlich in der Praxis umzusetzen**. Auch zeigen die Ergebnisse der Verbraucherbefragung sowie der beiden Praxistests, dass **Verbraucherinnen und Verbraucher differenzierte Einwilligungen und datensparsame Voreinstellungen überwiegend klar befürworten**. Und am Ende **profitieren auch die Unternehmen** von einer solchen Praxis: Denn die Verbraucherbefragung zeigt, dass **Verbraucherinnen und Verbraucher die Anbieter, die differenzierte Einwilligungsmodelle einsetzen, als wesentlich vertrauenswürdiger einschätzen als solche, die den Nutzerinnen und Nutzern keine Wahlmöglichkeiten lassen**.

Das Best Practice-Modell für EMS umfasst elf Anforderungen, die datenverarbeitenden Stellen dabei helfen sollen, die Vorgaben der Datenschutz-Grundverordnung sowohl rechtskonform als auch nutzerfreundlich umzusetzen. Die Anforderungen gliedern sich in drei Phasen: angefangen bei der Vorbereitung, über die Umsetzung eines Einwilligungsmodells bei der Erstanmeldung bis hin zur Umsetzung eines Datenschutz-Cockpits. Überdies sieht das Modell optionale Zusatzfunktionen vor.

Abstract

Consent is an essential instrument for the protection of privacy. In accordance with the General Data Protection Regulation, consent must be informed, differentiated and voluntary. In this light, consent management systems (CMS) are necessary to implement these requirements in a legally sound and user-friendly manner.

Against this background, the German Federal Ministry of Justice and Consumer Protection commissioned the research project "Innovative Data Protection Consent Management". The project analyzed existing CMS models in an online context, gathered consumer expectations in a representative online consumer survey with 2.029 participants as well as field studies with the two German companies Miele and Telekom. Finally, it developed recommendations for action to ensure legally compliant and user-friendly consent management in the form of a best practice-model.

The key finding of the study is that options exist to put the **requirements of the General Data Protection Regulation into practice in a legally compliant and user-friendly manner**. The results of the online representative consumer survey and the two practical tests also show that **most consumers clearly support differentiated consent and settings that focus on privacy by default**. Finally, **companies also benefit** from such a practice: The consumer survey shows that **consumers regard data processing entities who use differentiated CMS as much more trustworthy than those who do not let participants choose**.

The best practice model for CMS consists of eleven requirements which are intended to help data processing entities with implementing the requirements of the General Data Protection Regulation in a legally compliant and user-friendly manner. The requirements are divided into three phases: starting with preparation through the implementation of an initial consent management model to the implementation of a data protection cockpit. Furthermore, the model provides additional optional functions.

Vorbemerkungen und Danksagungen

Dieser Bericht fasst die inhaltlichen Ergebnisse des Forschungsvorhabens „Innovatives Datenschutz-Einwilligungsmanagement“ zusammen. Das Vorhaben wurde durch das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) durch das Bundesamt für Justiz (BfJ) im Zeitraum vom 01.07.2019 bis zum 15.05.2020 gefördert.

In diesem Zusammenhang möchten wir uns herzlich bei einer Vielzahl von Personen bedanken, die uns in den vergangenen Monaten bei der Umsetzung dieser Studie mit Ihrer Expertise und Ihren Hinweisen unterstützt haben. Hierzu bedanken wir uns bei den Teilnehmerinnen und Teilnehmern des Workshops am 04.12.2019, nämlich Lina Ehrig (vzbv), Denis Feth (Fraunhofer IESE), Sabine Frank (Google), Anja Hartmann (BfDI), Frank Ingenrieth (SRIW), Magnus Kowohl (Miele), Frederik Richter (Stiftung Datenschutz), Eva Schlehahn (ULD), Max Ulbricht (TU Berlin), Max von Grafenstein (UdK) und Rebekka Weiß (Bitkom). Des Weiteren danken wir Timo Jakobi (Universität Siegen), Armin Gerl (Universität Passau) und Hartmut Schmitt (HK Business Solutions) für ihre inhaltlichen Beiträge im Rahmen der Bestandsaufnahme.

Ein ganz herzlicher Dank gilt auch den Praxispartnern, ohne die eine Implementierung der Praxistests nicht möglich gewesen wäre und die einen erheblichen Zusatzaufwand auf sich genommen haben. Bei Miele & Cie. KG sind dies Jens Kohlenberg und Martin Löhe. Bei der Telekom Deutschland GmbH (Permission & übergreifendes Kundenmanagement) sind dies Carsten Akman und Marc Alexander Klisch sowie bei der Deutschen Telekom AG (Group Privacy) Susanne Eichhorn und Simone Wolf.

Inhaltsverzeichnis

1. Einleitung	12
1.1. Hintergrund	12
1.2. Zielsetzung und Forschungsfragen	13
1.3. Methodik	14
1.3.1. Bestandsaufnahme Literatur	15
1.3.2. Bestandsaufnahme Praxismodelle	15
1.3.3. Bestandsaufnahme Theorie-Modelle	16
1.3.4. Nutzerbefragung	16
1.3.5. Vorläufiger Anforderungskatalog, Überführung in ein theoretisches Modell und Validierung in einem Workshop	17
1.3.6. Praxistests	17
1.3.7. Ableitung des finalen Best Practice-Modells	18
2. Bestandsaufnahme Einwilligungsmodelle	19
2.1. Bewertungskriterien	19
2.1.1. Juristische Perspektive	19
2.1.2. Verhaltenswissenschaftliche Perspektive	43
2.2. Einwilligungsmanagementmodelle aus Praxis und Theorie	51
2.2.1. Praxisbeispiele für die Einwilligung bei Einzelanbietern	51
2.2.2. Beispiele aus der Theorie	59
2.2.3. Anbieterübergreifende Einwilligungsmanagementsysteme aus der Praxis	63
2.2.4. Mobile Umgebungen	66
2.2.5. Sonstige Funktionen	66
2.2.6. Zwischenfazit: Bislang gibt es nur sehr wenige differenzierte Einwilligungsmanagementsysteme in der Praxis – allerdings zeigen einige Good Practices, dass diese möglich sind	67
2.3. Bewertung der Einwilligungsmanagementmodelle aus Praxis und Theorie	68
2.3.1. Praxisbeispiele für die Einwilligung bei Einzelanbietern	68
2.3.2. Beispiele aus der Theorie	71
2.3.3. Anbieterübergreifende Einwilligungsmanagementsysteme aus der Praxis	72
2.3.4. Weitere, übergeordnete Aspekte und Bewertung sonstiger Funktionen	73
2.4. Vorläufige Handlungsempfehlungen	75
3. Exkurs: Cookie-Einwilligungsmodelle	77
3.1. Praxisbeispiele für die Cookie-Einwilligung bei Einzelanbietern	79
3.1.1. Keine Wahl oder globale Einwilligung	79
3.1.2. Binäre Wahl	79
3.1.3. Differenzierte Cookie-Einwilligung	80
3.2. Praxisbeispiele für die globale Cookie-Einwilligung	82
3.2.1. Differenzierter und globaler Opt-Out	82
3.2.2. Browser Plugins	83
3.3. Bewertung der Modelle	84

3.3.1. Praxisbeispiele für die Cookie-Einwilligung	84
3.3.2. Praxisbeispiele für die globale Cookie-Einwilligung	85
3.3.3. Weitere, übergeordnete Aspekte und Bewertung sonstiger Funktionen	86
4. Nutzerbefragung	88
4.1. Bewertung von Einwilligungsmodellen aus Nutzerperspektive	88
4.1.1. Gesamtbewertung der Modelle	92
4.1.2. Anpassungsmöglichkeiten	93
4.1.3. Vertrauen in den Anbieter	94
4.1.4. Informiertheit	95
4.1.5. Einfachheit	96
4.1.6. Übersichtlichkeit	97
4.1.7. Zusammenfassung	99
4.2. Vergleich unterschiedlicher Gestaltungsparameter	100
4.2.1. Präferenzen zu Voreinstellungen	100
4.2.2. Präferenzen zum gewünschten Grad der Differenzierung	102
4.2.3. Präferenzen zur gewünschten Menge der Informationen	105
4.2.4. Zusammenfassung	107
4.3. Präferenzen zu Zusatzfunktionen	108
4.4. Weitere Ergebnisse	109
5. Praxistests	113
5.1. Praxistest „Einwilligung“ (Miele)	113
5.1.1. Einwilligungsmodell: Gesamtbewertung	114
5.1.2. Einwilligungsmodell: Anpassungsmöglichkeiten	115
5.1.3. Einwilligungsmodell: Vertrauen in den Anbieter	116
5.1.4. Einwilligungsmodell: Informiertheit	117
5.1.5. Einwilligungsmodell: Einfachheit	118
5.1.6. Einwilligungsmodell: Potentielle Nutzung	119
5.1.7. Zusammenfassung	119
5.2. Praxistest „Einwilligungsmanagement in Nachhinein“ (Telekom)	120
5.2.1. Version A: Status Quo	120
5.2.2. Version B: Erweiterung mit Datenschutz-Cockpit	121
5.2.3. Überblick über die Bewertung und Vergleich beider Modelle	122
5.2.4. Nutzung des InfoService: Anpassungsmöglichkeiten	122
5.2.5. Nutzung des InfoService: Vertrauen in den Anbieter	123
5.2.6. Nutzung des InfoService: Übersichtlichkeit	123
5.2.7. Nutzung des InfoService: Verständlichkeit	124
5.2.8. Nutzung des InfoService: Hilfe	124
5.2.9. Nutzung des InfoService: Mehrwert	124
5.2.10. Zusammenfassung	125
6. Best Practice-Modell	126
6.1. Vorbereitungsphase (A)	128
6.1.1. Anforderungen	128
6.1.2. Vorbereitungsphase: Illustration der Umsetzung	130
6.2. Umsetzungsphase Einwilligung (B)	132
6.2.1. Anforderungen	132
6.2.2. Illustration der Umsetzung	135

6.3. Umsetzungsphase Management der Einwilligung (C)	138
6.3.1. Anforderungen	138
6.3.2. Illustration der Umsetzung	139
6.4. Optionale Zusatzfunktionen	141
6.4.1. Anforderungen	141
6.4.2. Illustration der Umsetzung	142
6.5. User Journey: Mock-Ups der Umsetzung	143
7. Literatur	150
8. Anhang	157
Anhang A: Befragungskonzept Verbraucherbefragung	157
A.1. Mock-Ups Modell v1 (globale Einwilligung)	157
A.2. Mock-Ups Model v2 (erzwungene Einwilligung)	159
A.3. Mock-Ups Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups)	161
A.4. Mock-Ups Modell v4 (Differenzierung ohne Auswahl und mit Erläuterungstext)	163
A.5. Fragestellungen Zusatzfunktionen	166
Anhang B: Befragungskonzept Praxistest Miele	168
B.1. Screenshots	168
B.2. Fragebogen zum Modell	174
Anhang C: Befragungskonzept Praxistest Telekom	176
C.1. Version A (Status Quo)	176
C.2. Version B (Datenschutz-Cockpit)	177

Abkürzungsverzeichnis

BGH	Bundesgerichtshof
DI-RL	EU-Richtlinie zur Bereitstellung digitaler Inhalte und digitaler Dienstleistungen
DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)
EDAA	European Interactive Digital Advertising Alliance
EDSA	Europäischer Datenschutzausschuss
EMIDD	Einwilligungsmanagement für das Internet der Dinge
ErwGr	Erwägungsgrund
EuGH	Europäischer Gerichtshof
HCD	Human Centered Design
LPL PPP UI	Layered Privacy Language Personal Privacy Policy User Interface
PIMS	Personal Information Management Services
PMT	Privacy Management Tools
RL	Richtlinie
Telekom	Beteiligte Institutionen im Praxistests sind Telekom Deutschland GmbH (Permission & übergreifendes Kundenmanagement) und Deutsche Telekom AG (Group Privacy)
TMG	Telemediengesetz
UX	User Experience
vzbv	Verbraucherzentrale Bundesverband

Abbildungsverzeichnis

Abbildung 1: Beispiel für Vertrauens-Frame	45
Abbildung 2: Beispiel für Experten-Frame	46
Abbildung 3: Beispiel für wechselnde Formulierungen	46
Abbildung 4: Beispiel für Voreinstellungen	47
Abbildung 5: Beispiel für Wahloption ohne Voreinstellung (1/2)	47
Abbildung 6: Differenzierungsmöglichkeiten und Bewertung durch Verbraucherinnen und Verbraucher	50
Abbildung 7: Beispiel für voreingestellte Datenverarbeitung mit Knöpfen („zugestimmt“)	53
Abbildung 8: Beispiel für voreingestellte Datenverarbeitungen mit Buttons (Google)	54
Abbildung 9: Beispiel für voreingestellte Datenverarbeitung mit Check-Boxen ("nicht zugestimmt")	55
Abbildung 10: Beispiel für voreingestellte Datenverarbeitung mit Check-Boxen (openSAP)	56
Abbildung 11: Beispiel für eine Wahloption ohne Voreinstellung (2/2)	57
Abbildung 12: Beispiel für Einwilligungsmanagement im Nachhinein (1/2) (Google My Account)	58
Abbildung 13: Beispiel für Einwilligungsmanagement im Nachhinein (2/2) (Google My Account)	59
Abbildung 14: Demonstrator des LPL PPP UI-Modells (Gerl & Prey, 2018)	60
Abbildung 15: Demonstrator des EMIDD-Modells (Ulbricht & Pallas, 2018)	61
Abbildung 16: Demonstrator des SPECIAL Consent and control 2-Modells (SPECIAL, 2018)	62
Abbildung 17: Demonstrator des SPECIAL Consent and control 3-Modells (Drozd & Kirrane, o.D.)	63
Abbildung 18: Beispiel für PIMS (digi.me)	64
Abbildung 19: Schematische Darstellung eines PIMS (it's my data)	65
Abbildung 20: Beispiel für übergreifendes Einwilligungsmanagementsystem (Cliqz re:consent)	65
Abbildung 21: Beispiel für bildliche Unterermalung von Datenschutztexten (Datenverarbeitung, Datenweitergabe und Tracking, Xing)	66
Abbildung 22: Beispiel für bildliche Unterermalung von Datenschutztexten (Standortdaten, Google)	66
Abbildung 23: Beispiel für die Verbildlichung von Datenströmen (SPECIAL Projekt)	67
Abbildung 24: Beispiel für binäre Einstellung von Cookies	79
Abbildung 25: Beispiel für Cookie-Banner bei dem alle Kategorien vorausgewählt sind (digi.me)	80
Abbildung 26: Beispiel für Cookie-Banner mit Menüführung und inaktiven Cookies (OneTrust)	80
Abbildung 27: Beispiel für Oberfläche zur Einstellung von Cookies mit unterschiedlichen Voreinstellungen (usercentrics)	81

Abbildung 28: Beispiel für Oberfläche zur Einstellung von Cookies mit unterschiedlichen Voreinstellungen (consentmanager)	81
Abbildung 29: Beispiel für Cookie-Banner mit voreingestellter Datenverarbeitung („inaktiv“) und Check-Boxen (Belgian Train)	82
Abbildung 30: Beispiel für globales Cookie-Management (Your Online Choices)	82
Abbildung 31: Beispiel für Browser Plugin zum Cookie-Management (Ghostery)	83
Abbildung 32: Beispiel für Browser Plugin zum Cookie-Management (Privacy Badger)	83
Abbildung 33: Beispiel für Cookie-Banner mit positiver Rahmung (Oreo)	87
Abbildung 34: Beispiel für Cookie-Einstellungen mit Empfehlung	87
Abbildung 35: Befragungsdesign von Modell v1 (globale Einwilligung) auf drei Bildschirmen	89
Abbildung 36: Befragungsdesign von Modell v2 (erzwungene Einwilligung) auf vier Bildschirmen	89
Abbildung 37: Befragungsdesign von Modell v3 (differenzierte Einwilligung mit Voreinstellung und Pop-Ups) auf fünf Bildschirmen	90
Abbildung 38: Befragungsdesign von Modell v4 (differenzierte Einwilligung mit Check-Boxen und Erläuterungen im Hauptfenster) auf fünf Bildschirmen	91
Abbildung 39: Befragungsergebnisse zur Gesamtbewertung der Einwilligungsmodelle	92
Abbildung 40: Befragungsergebnisse zur Anpassungsmöglichkeit der Einwilligungsmodelle	94
Abbildung 41: Befragungsergebnisse zur Vertrauenswürdigkeit der Einwilligungsmodelle	95
Abbildung 42: Befragungsergebnisse zur Informiertheit durch die Einwilligungsmodelle	96
Abbildung 43: Befragungsergebnisse zur Einfachheit der Einwilligungsmodelle	97
Abbildung 44: Befragungsergebnisse zur Übersichtlichkeit der Einwilligungsmodelle	98
Abbildung 45: Befragungsdesign "Voreinstellungen"	101
Abbildung 46: Befragungsergebnisse – keine Voreinstellung vs. Voreinstellung "nicht zugestimmt"	101
Abbildung 47: Befragungsergebnisse – keine Voreinstellung vs. Voreinstellung "zugestimmt"	101
Abbildung 48: Befragungsergebnisse - Voreinstellung "nicht zugestimmt" vs. Voreinstellung "zugestimmt"	102
Abbildung 49: Befragungsdesign „Grad der Differenzierung“	103
Abbildung 50: Befragungsergebnisse – keine Differenzierung vs. mittlere Differenzierung	103
Abbildung 51: Befragungsergebnisse – keine Differenzierung vs. starke Differenzierung	104
Abbildung 52: Befragungsergebnisse – mittlere Differenzierung vs. starke Differenzierung	104
Abbildung 53: Befragungsdesign „Menge der Informationen“	105

Abbildung 54: Befragungsergebnisse – keine Erklärung vs. zusätzliche Erklärung immer angezeigt	106
Abbildung 55: Befragungsergebnisse – keine Erklärung vs. zusätzliche Erklärung in Pop-Up	106
Abbildung 56: Befragungsergebnisse – zusätzliche Erklärung in Pop-Up vs. zusätzliche Erklärung immer angezeigt	107
Abbildung 57: Befragungsergebnisse zu Zusatzfunktionen	109
Abbildung 58: Befragungsergebnisse zum Anzeigzeitpunkt der Datenschutztexte	109
Abbildung 59: Befragungsergebnisse zum mangendeln Leseverhalten von Verbraucherinnen und Verbrauchern	111
Abbildung 60: Befragungsergebnisse zur Nutzung von Diensten ohne zusätzliche Datenverarbeitung	111
Abbildung 61: Befragungsergebnisse zur Einwilligung in nicht erforderliche Daten	112
Abbildung 62: Ergebnis Praxistest "Einwilligung" zur Gesamtbewertung des Modells	114
Abbildung 63: Ergebnis Praxistest "Einwilligung" zur Anpassungsmöglichkeit des Modells	115
Abbildung 64: Ergebnis Praxistest "Einwilligung" zur Bewertung der Einstellungsmöglichkeiten des Modells	116
Abbildung 65: Ergebnis Praxistest "Einwilligung" zur Vertrauenswürdigkeit des Modells	117
Abbildung 66: Ergebnis Praxistest "Einwilligung" zur Informiertheit durch das Modell	117
Abbildung 67: Ergebnis Praxistest "Einwilligung" zur Einfachheit des Modells	118
Abbildung 68: Ergebnis Praxistest "Einwilligung" zur potentiellen Nutzung des Modells	119
Abbildung 69: Design Praxistest "Einwilligungsmanagement im Nachhinein" - InfoService Status Quo (Version A)	121
Abbildung 70: Design Praxistest „Einwilligungsmanagement im Nachhinein“ – Neuer InfoService als Datenschutz-Cockpit (Version B)	121
Abbildung 71: Ergebnis Praxistest „Einwilligungsmanagement im Nachhinein“ zum Überblick über die Bewertung und Vergleich der Modelle	122
Abbildung 72: Entscheidungsbaumlogik für komplexere Datenverarbeitungen	132
Abbildung 73: Best Practice-Modell – Mock-Ups "Datensparsame Voreinstellungen"	136
Abbildung 74: Best Practice-Modell – Mock-Ups "Erläuternde Texte in Pop-Ups"	137
Abbildung 75: Best Practice-Modell – Mock-Ups "Datensparsame Voreinstellungen" und "Erläuternde Texte in Pop-Ups" (Mobile Endgeräte)	137
Abbildung 76: Best Practice-Modell – Mock-Ups "Auswahl der Datenschutz-Einstellungen" in komplexeren Systemen (Stufe 1)	138
Abbildung 77: Best Practice-Modell – Mock-Ups "Datenschutz-Cockpit"	140
Abbildung 78: Best Practice-Modell – Mock-Ups "Datenschutz-Cockpit" (Mobile Endgeräte)	141

Tabellenverzeichnis

Tabelle 1: Befragungsdesign Anzahl der Observationen je Modell	92
Tabelle 2: Zusammenfassung der Modellbewertungen nach Anteil der positiven Bewertungen über die Bewertungsdimensionen	99
Tabelle 3: Zusammenfassung der Modellbewertungen und Rangreihenfolge über die Bewertungsdimensionen	100
Tabelle 4: Illustration der Umsetzung des Best Practice-Modells – Datenarten und Zwecke	131

1. Einleitung

1.1. Hintergrund

Seit Mai 2018 gilt die Datenschutz-Grundverordnung (DS-GVO), die die Rechte der Verbraucherinnen und Verbraucher bei der Erhebung und Verarbeitung ihrer personenbezogenen Daten stärkt. Die DS-GVO sieht neben umfangreichen Transparenzpflichten vor, dass die Einwilligung in Datenverarbeitungen *freiwillig* und *informiert* geschieht und *differenzierte Einwilligungen* ermöglicht werden. Damit diese differenzierten Einwilligungsmöglichkeiten praktisch umgesetzt werden, sind innovative Einwilligungsmanagement-Systeme nötig, die sowohl nutzerfreundlich gestaltet als auch rechtssicher sind.

Die differenzierte Einwilligung zielt darauf ab, Verbraucherinnen und Verbrauchern mehr Kontrolle im Umgang mit ihren Daten zu geben. Jedoch zeigen Umfragen, dass diese Datenkontrolle oftmals im Argen liegt. In einer Befragung der Europäischen Kommission gaben lediglich 4% der Befragten aus Deutschland an, dass sie eine vollständige Kontrolle über ihre Daten haben; 45% gaben hingegen an, dass sie überhaupt keine Datenkontrolle besäßen, wobei hiervon 68% berichteten, dass sie über die mangelnde Kontrolle beunruhigt seien.¹ Auch kommt ein Rechtsgutachten des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) zu dem Ergebnis, dass es bei den im Rahmen der Studie untersuchten Unternehmen noch „erhebliche Probleme bei der Umsetzung einer datenschutzkonformen Einwilligung“ gibt.²

In der Praxis existieren seit Inkrafttreten der DS-GVO bereits einige Beispiele von Einwilligungsmanagement-Systemen, die eine Differenzierung bei der Erhebung von personenbezogenen Daten in Einwilligungsprozessen oder bei der Nutzung von Cookies vorsehen. Diese Einstellungsmöglichkeiten bieten Nutzerinnen und Nutzern mehr Wahlfreiheit, jedoch besteht ein Risiko darin, dass die Praktikabilität dieser Lösung mit der Anzahl der Einstellungsmöglichkeiten sinkt: D.h. je mehr Entscheidungen Verbraucherinnen und Verbraucher treffen müssen, desto aufwändiger könnte dies für sie sein. Zu einem ähnlichen Ergebnis kommt die wissenschaftliche Literatur zur „Choice Overload“-Hypothese. Diese Hypothese besagt, dass mit einer steigenden Anzahl an Auswahloptionen nachteilige Konsequenzen einhergehen können, die dazu führen, dass Verbraucherinnen und Verbraucher weniger motiviert sind, Entscheidungen zu treffen. Im ungünstigsten Fall kann dies dazu führen, dass Verbraucherinnen und Verbraucher aufgrund der Überlastung suboptimale Entscheidungen treffen.³

Diesen negativen Effekten könnte durch Voreinstellungen entgegengewirkt werden, indem bspw. „per Default“ nur notwendige Daten erhoben werden. Das Vorgehen in der Realität ist jedoch häufig ein anderes.

¹ Special Eurobarometer 431. (2015). Data protection. Abgerufen von https://data.europa.eu/eu-odp/de/data/dataset/S2075_83_1_431_ENG (18.04.2019)

² Wiebe, A., Helmschrot, C. (2019). Untersuchung der Umsetzung der Datenschutz-Grundverordnung (DSGVO) durch Online-Dienste. Studie im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz, S. 242.

³ Scheibehenne, B., Greifeneder, R., & Todd, P. M. (2010). Can there ever be too many options? A meta-analytic review of choice overload. *Journal of Consumer Research*, 37(3), 409-425.

Eine Studie der Stiftung Datenschutz aus dem Jahr 2017 kommt zu dem Schluss, dass sich *technische Lösungen* für das Einwilligungsmanagement anbieten, die es Verbraucherinnen und Verbrauchern ermöglichen, ihre Daten automatisiert zu managen.⁴ Auch die Datenethikkommission sieht in innovativen Datenmanagement- und Treuhandsystemen ein großes Potential.⁵ Jedoch finden diese sogenannten „Privacy Management Tools“ (PMT) und „Personal Information Management Services“ (PIMS) in der Unternehmenspraxis bisher kaum Anwendung und wurden noch nicht systematisch auf ihre Wirksamkeit überprüft.

Darüber hinaus wurde noch nicht systematisch empirisch untersucht, welche Erwartungen Verbraucherinnen und Verbraucher an Systeme zur Erhebung und Koordinierung ihrer Einwilligungen haben. So ist bspw. unklar, welche informatorische Unterstützung notwendig ist, welche Assistenzfunktionen ein solches System haben sollte und wie die Nutzung praktikabel umgesetzt werden sollte.

1.2. Zielsetzung und Forschungsfragen

Vor diesem Hintergrund besteht das übergeordnete Ziel des Forschungsvorhabens darin, bereits vorhandene Modelle zum Einwilligungsmanagement zu analysieren und im Ergebnis neue Lösungsansätze zur rechtskonformen und nutzerfreundlichen Einwilligung zu entwickeln. Um dieses Ziel zu erreichen, wurden innerhalb des Untersuchungszeitraums von Juli 2019 bis Juni 2020 insgesamt sechs Arbeitsschritte umgesetzt: Im ersten Schritt wurde eine Bestandsaufnahme der Umsetzung von Einwilligungsmanagement-Systemen in der Theorie und Praxis durchgeführt (Kapitel 2 bis 3). Zweitens wurde im Rahmen einer repräsentativen Online-Verbraucherbefragung untersucht, welche Erwartungen Verbraucherinnen und Verbraucher an Systeme zur differenzierten Einwilligung haben (Kapitel 4). Darauf aufbauend wurden Empfehlungen für neue Lösungsansätze für nutzerfreundliche und rechtssichere Einwilligungsmanagement-Systeme entwickelt und in ein theoretisches Konzept überführt. Hieran schloss sich eine empirische Untersuchung des Konzepts in zwei Praxistests an (Kapitel 5). Im letzten Schritt wurden die Ergebnisse konsolidiert und ein finales Best Practice-Modell abgeleitet (Kapitel 6).

Im Konkreten werden im Rahmen des Vorhabens folgende Forschungsfragen systematisch beantwortet:

Bestandsaufnahme

- Welche Einwilligungsmanagement-Systeme gibt es in der Theorie, d.h. wissenschaftlichen und grauen Literatur? Welche in der Praxis?

⁴ Horn, N., Riechert, A. & Müller, C. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Stiftung Datenschutz. Abgerufen von https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf (18.04.19)

⁵ Datenethikkommission (2019). Gutachten der Datenethikkommission. Abgerufen von: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=D320786A39EF7EA4BCD184251FE7831A.1_cid364?_blob=publicationFile&v=6 (15.03.2020)

- Wie sind diese Systeme und die zugehörigen Nutzerführungskonzepte sowie Einzelfunktionen gestaltet?
- Wie schneiden die Systeme im Hinblick auf rechtliche und verhaltenswissenschaftliche Aspekte ab?
- Welche Vor- und Nachteile haben die Systeme?
- Welche Einzelfunktionen sind empfehlenswert?
- Welche konkreten Verbesserungspotentiale gibt es?

Erwartungen und Forderungen der Verbraucherinnen und Verbraucher

- Welche allgemeinen und konkreten Erwartungen haben Verbraucherinnen und Verbraucher an ein Einwilligungsmanagement-System?
- Gibt es Unterschiede zwischen Bevölkerungsgruppen oder Nutzertypen?

Empfehlungen und Kriterien für ein innovatives Einwilligungsmanagement-System

- Welche Mindestanforderungen muss ein innovatives Einwilligungsmanagement-System erfüllen?
- Welche rechtlichen Aspekte müssen hierbei beachtet werden?
- Welche Anforderungen an die Nutzerfreundlichkeit und Praktikabilität existieren?

Erstellung eines theoretischen Modells für innovatives Einwilligungsmanagement

- Wie sieht ein idealtypisches Modell aus, das rechtskonform und nutzerfreundlich ist?
- Welche freien und fixen Parameter gibt es in der Gestaltung?
- Wie kann das Modell in der Praxis umgesetzt werden?
- Welche Anpassungen sind für unterschiedliche Zielgruppen oder Endgeräte notwendig?

Testung des theoretischen Modells in der Praxis

- Wie schneidet das Modell in einem Praxistest ab?
- Verbessert es tatsächlich die Einwilligungssituation für Verbraucherinnen und Verbraucher?

1.3. Methodik

Insgesamt speisen sich die Studienergebnisse aus sieben Quellen: Erstens wurde die wissenschaftliche und graue Literatur untersucht. Zweitens wurden Praxismodelle identifiziert und durch die Dokumentation der jeweiligen Customer Journeys ausgewertet. Drittens wurden Theoriemodelle recherchiert und analysiert. Im vierten Schritt wurden quantitative Verbraucherdaten in einer bevölkerungsrepräsentativen Online-Befragung erhoben. Aus diesen Ergebnissen wurden im fünften Schritt vorläufige Anforderungen abgeleitet und in einem

Workshop validiert. Sechstens wurden konkrete Modelle erstellt und in zwei Praxistests an Nutzerinnen und Nutzern getestet. Im siebten und letzten Schritt wurde das finale Best Practice-Modell abgeleitet, das die Anforderungen aller vorhergehenden Schritte synthetisiert. Die folgenden Abschnitte erläutern die methodische Umsetzung.

1.3.1. Bestandsaufnahme Literatur

Im ersten Schritt der Bestandsaufnahme wurde die **wissenschaftliche und graue Literatur** durchsucht und dokumentiert. Sowohl für die rechtswissenschaftliche als auch für die verhaltenswissenschaftliche Literaturanalyse wurde methodisch zunächst eine umfassende Suche in einschlägigen wissenschaftlichen Literaturdatenbanken durchgeführt und die dort identifizierten Peer-reviewed Publikationen ausgewertet. Weiterhin wurden Datenbanken öffentlicher Institutionen (wie Europäische Kommission), Forschungsinstitute (wie DIW) sowie relevanter Akteure im Online-Bereich (wie Bitkom oder AK Usable Security & Privacy der German UPA) nach Forschungs- und Projektergebnissen gesichtet.

Da es für bestimmte Forschungsprojekte bisher keine Veröffentlichungen gibt, diese jedoch relevant für die Bestandsaufnahme sein könnten, wurde zusätzlich eine **Expertenabfrage** umgesetzt. Hierfür wurden Expertinnen und Experten aus dem Bereich Datenschutz und Usability angeschrieben, um Hinweise auf weitere Modellbeispiele sowie unveröffentlichte Forschungsvorhaben zu erhalten.

1.3.2. Bestandsaufnahme Praxismodelle

Um die Customer Journey, d.h. die Schritte, die zum Abschließen eines Prozesses durchlaufen werden, in der Realität nachzuempfinden, wurde mit einer funktionalen Email-Adresse bei ausgewählten Diensten eine Anmeldung vollzogen und der **Anmeldeprozess** dokumentiert. Für die Anmeldungen wurde einheitlich der von vielen Verbraucherinnen und Verbrauchern genutzte Browser Google Chrome genutzt.⁶

Insgesamt wurden zwölf vollständige Anmeldungen durchgeführt und hierbei die folgenden Dienstleistungen berücksichtigt:⁷

- E-Mail-Dienste
- Online-Shops
- Soziale Netzwerke
- Vergleichsportale
- Unternehmen aus dem Mobilitäts- und Cloudbereich

⁶ Der Google Chrome Browser wurde gewählt, da er in Deutschland mit 47% die höchsten Marktanteile aufweist (vgl. Daten von statcounter (2019) Desktop Browser Market Share Germany – Jan 2009 – July 2019. Abgerufen von: <https://gs.statcounter.com/browser-market-share/desktop/germany/#monthly-200901-201907> (26.07.2019))

⁷ Die Dienstleistungskategorien orientieren sich hierbei grob an denen, die für das BMJV-Forschungsvorhaben „DSGVO-Check“ von der Universität Göttingen (Prof. Wiebe) bearbeitet wurden.

Zusätzlich wurde für die Dienste die Customer Journey zur Anmeldung in einer **mobilen Umgebung** wiederholt. Hierfür wurden die Anmeldeschritte auf einem Android Smartphone im Google Chrome Browser durchgeführt und mit Screenshots dokumentiert.

Überdies wurden auch sog. **PIMS** und **Consent Management Platforms** gesichtet. Da diese jedoch nicht im realen Nutzungsbetrieb betrachtet werden konnten, da die Anbieter sie lediglich für Unternehmenskunden implementieren, wurden die Lösungen lediglich auf Grundlage der Webseiten-Informationen dokumentiert, nicht jedoch in einer vollständigen Customer Journey getestet.

Darüber hinaus wurde auf selektierten Nachrichten- und Informationsportalen die Customer Journey zur **Anpassung von Webseiten-Cookies** vollzogen und dokumentiert. Hierfür war keine reale Anmeldung notwendig.

Auch existieren für den Browser Firefox sog. Plugins, d.h. Zusatzmodule bzw. Software-Erweiterungen, die für das **Cookie-Management** genutzt werden können. Insgesamt wurden zwei solcher Plugins installiert und die reale Nutzung dokumentiert.

Es ist zu betonen, dass die ausgewählten Dienste nicht repräsentativ für die gesamte Dienstleistungslandschaft im Internet sind. An dieser Stelle sei auf das Gutachten von Wiebe und Helmschrot (2019) verwiesen, das sich konkret mit der Auswertung von Online-Diensten mit Blick auf ihre Datenschutzpraktiken befasst. Neben relevanten Diensten, die eine hohe Marktabdeckung haben und eine hohe Reichweite besitzen, wurden zusätzlich auch Best Practice-Beispiele ausgesucht, die zwar eine niedrigere Reichweite besitzen, aber besondere Maßnahmen bei der Einwilligung ergreifen.

1.3.3. Bestandsaufnahme Theorie-Modelle

Zusätzlich zu den Praxismodellen wurden in der Bestandsaufnahme auch **theoretische Modelle** aus Forschungsprojekten berücksichtigt. Eine Dokumentation der Customer Journey war hierbei nur begrenzt möglich, da diese nicht in einer realen Anwendung genutzt werden können. Die vorgesehenen Anmeldeschritte sowie vorgesehene Funktionen der Modelle wurden deshalb lediglich schriftlich dokumentiert.

1.3.4. Nutzerbefragung

Um die **Wünsche und Erwartungen** von Verbraucherinnen und Verbrauchern zu erheben, wurde eine repräsentative Online-Befragung durchgeführt. Hierbei wurden den Teilnehmerinnen und Teilnehmern reale Einwilligungsmodelle mit Mock-Ups zur Bewertung vorgestellt, die auf den Modellen aus der Bestandsaufnahme beruhen. Darüber hinaus wurden die Präferenzen der Verbraucherinnen und Verbraucher bezüglich unterschiedlicher Ausgestaltungsformen beim Differenzierungsumfang, der Informationsmenge und den Voreinstellungen untersucht und das Interesse für weitere datenschutzrelevante Funktionen erhoben. Weitere Informationen zum Befragungskonzept finden sich in Anhang A.

Die verwendeten Daten beruhen auf einer **Online-Umfrage** der YouGov Deutschland GmbH, an der 2.029 Personen zwischen dem 06. und 09. September 2019 teilnahmen. Die Ergebnisse wurden gewichtet und sind repräsentativ für die deutsche Bevölkerung ab 18 Jahren.

1.3.5. Vorläufiger Anforderungskatalog, Überführung in ein theoretisches Modell und Validierung in einem Workshop

Aus den bisherigen Ergebnissen wurde ein vorläufiger Anforderungskatalog abgeleitet. Hierbei wurden sowohl rechtliche Vorgaben als auch solche an die Nutzerfreundlichkeit und Praktikabilität berücksichtigt.

Danach wurde der entwickelte Anforderungskatalog in ein theoretisches Modell überführt und in einem Workshop diskutiert und validiert. Der **Workshop** fand am 4. Dezember 2019 im Bundesministerium der Justiz und für Verbraucherschutz in Berlin statt. Es nahmen Vertreterinnen und Vertreter aus Politik, Aufsichtsbehörden, Wirtschaft, Verbänden, Wissenschaft und Zivilgesellschaft daran teil. Ziel des Workshops war es zum einen, die Ergebnisse der Bestandsaufnahme und der Befragung zu diskutieren. Zum anderen wurden die vorläufigen Mock-Ups der Modelle, die in den Praxistests bei Miele Cie. & KG (im folgenden Miele) und der Deutsche Telekom AG mit der Telekom Deutschland GmbH (im folgenden Telekom) getestet werden sollten, diskutiert.

1.3.6. Praxistests

Das Feedback aus dem Workshop wurde sodann genutzt, um die Praxismodelle weiterzuentwickeln. Die beiden Praxistests fanden dann im 1. Quartal 2020 statt und wurden bei Miele und der Telekom umgesetzt.

Bei Miele wurde ein **Einwilligungsmodell** zur Erstanmeldung erprobt. Die Testung fand innerhalb der MyMiele-Community statt und es nahmen N=37 Kundinnen und Kunden daran teil. Im Anschluss an das präsentierte Modell wurden Bewertungsfragen zur Nutzung und Bedienbarkeit gestellt. Weitere Informationen zum Befragungskonzept finden sich im Anhang B.

Bei der Telekom wurde das Datenschutzmanagement im Nachhinein untersucht und unterschiedliche Einwilligungsmodelle gegeneinander getestet. Dabei wurde auch ein **Datenschutz-Cockpit** erprobt.⁸ An der Testung, die in einem Online-Panel umgesetzt wurde, nahmen N=906 Kundinnen und Kunden teil. Im Anschluss an die vorgestellten Modelle, die einem realen Kaufprozess nachempfunden waren, wurde ein Fragebogen zur Nutzung und Praktikabilität der Modelle gestellt. Weitere Details zur Befragung finden sich im Anhang C.

⁸ Der Begriff des Datenschutz-Cockpits beschreibt im Rahmen der Studie eine Anwendungsoberfläche, in der Nutzerinnen und Nutzer ihre Einwilligungen einsehen können. Darüber hinaus ermöglicht das Cockpit den Nutzerinnen und Nutzern – in Anlehnung an die Steuerung eines Flugzeuges – aktiv und autonom die Steuerung darüber zu übernehmen, welche Daten für welche Zwecke verarbeitet werden dürfen. Dabei ist das Datenschutz-Cockpit also von einem Datenschutz-Dashboard abzugrenzen, da letzteres lediglich eine Transparenzfunktion übernimmt und Nutzerinnen und Nutzern anzeigt, welche Daten verarbeitet werden, nicht jedoch Einstellungsmöglichkeiten bietet.

1.3.7. Ableitung des finalen Best Practice-Modells

Nachdem alle Ergebnisse vorlagen, wurde das **finale Best Practice-Modell** abgeleitet. Dabei wurde der Gesamtprozess inklusive aller Vorbereitungs- und Umsetzungsschritte anhand eines fiktiven Unternehmens illustriert. Die gestalterische Umsetzung findet sich darüber hinaus in Mock-Ups, sog. Attrappen zur Visualisierung der Designparameter wieder.

2. Bestandsaufnahme Einwilligungsmodelle

Die Studie zielt darauf ab, neue Lösungsansätze zur rechtskonformen und nutzerfreundlichen Einwilligung zu entwickeln. Hierfür ist es in einem ersten Schritt notwendig, eine Bestandsaufnahme durchzuführen. Zunächst werden in dieser Bestandsaufnahme die Bewertungskriterien für Einwilligungsmanagementmodelle (Abschnitt 2.1) hergeleitet. Hiernach werden Modelle aus der Praxis und Theorie (Abschnitt 2.2) beschrieben und im letzten Schritt eine Bewertung der Modelle vorgenommen (Abschnitt 2.3). Abschließend werden vorläufige Handlungsempfehlungen abgeleitet (Abschnitt 2.4).

2.1. Bewertungskriterien

Zur Festlegung der Bewertungskriterien wurde zum einen die rechtswissenschaftliche Literatur analysiert und die Voraussetzungen für ein rechtskonformes Einwilligungsmanagement wurden definiert. Diese werden in Abschnitt 2.1.1 beschrieben. Zusätzlich wurden verhaltenswissenschaftliche Kriterien aus der Literatur abgeleitet, die in Abschnitt 2.1.2 vorgestellt werden.

2.1.1. Juristische Perspektive

Um beurteilen zu können, wie eine Einwilligung datenschutzkonform und nutzerfreundlich dargestellt, gestaltet und strukturiert werden sollte, insbesondere welche Merkmale ein innovatives Einwilligungsmanagement aus juristischer Perspektive auszeichnen (mit besonderem Blick auf ein Smartphone und/oder Tablet), erfordert es eine eingehende Untersuchung der Wirksamkeitsvoraussetzungen der Einwilligung.

Hierzu werden in einem ersten Schritt die formellen Voraussetzungen der Einwilligung (in Abhängigkeit des Verarbeitungskontextes) skizziert (2.1.1.2). Sodann erfolgt eine Analyse der materiellen Voraussetzungen, die Ausgangspunkt der informationellen Selbstbestimmung sind (Informiertheit, Einzelfallbezogenheit und Freiwilligkeit) (2.1.1.3 ff.). Schlussendlich werden unterschiedliche Einwilligungsmechanismen untersucht und herausgearbeitet, ob und wie ein (ggf. zentralisiertes) Einwilligungsmanagementsystem als innovativer, datenschutzkonformer Erteilungs- und Widerrufsmechanismus in Frage kommt (2.1.1.7).

Die DS-GVO⁹ entwickelt in den Artt. 4 – 9 DS-GVO die Grundlagen der datenschutzrechtlichen Einwilligung. Die derzeit (noch) geltende e-Privacy-Richtlinie¹⁰ verweist hinsichtlich „ihrer“ Einwilligung i. R. d. elektronischen Kommunikation

⁹ 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, ABl. L 119 vom 04.05.2016, S. 1–88.

¹⁰ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 201 vom 31.07.2002, S. 37–47 i.d. zuletzt geänderten Fassung v. 19. Dezember 2009.

(Art. 5 Abs. 3 e-Privacy-RL) in Art. 2 lit. f e-Privacy-RL auf die Einwilligungsvoraussetzungen der Datenschutzrichtlinie.¹¹ Dieser Verweis auf die Vorgaben der ehemalige DS-RL ist gem. Art. 94 Abs. 2 S. 1 DS-GVO nunmehr als Verweis auf die DS-GVO zu verstehen, sodass die folgenden Ausführungen gleichsam auch für die e-Privacy-RL gelten.¹² Nichts anderes gilt nach heutigem Kenntnisstand auch für die künftige, sich im Entwurf befindliche e-Privacy-Verordnung,¹³ s. ErwGr 3 S. 3 u. 4 e-Privacy-VO-E.

2.1.1.1. Anforderungen an die Einwilligung nach Art. 4, Art. 7 DS-GVO

Die Voraussetzungen für eine wirksame Einwilligung ergeben sich aus Artt. 4 und 6 – 9 DS-GVO sowie der zugehörigen Erwägungsgründe. Artikel 4 Absatz 11 der DS-GVO definiert die Einwilligung als

„jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.

Maßgeblich sind daher:¹⁴

- die Freiwilligkeit
- eine angemessene Informiertheit in Folge einer ausreichenden Informationsgrundlage
- eine eindeutige, unmissverständliche und aktive Bestätigungshandlung
- der Bezug auf einen bestimmten Fall

Zusätzlich muss der Datenverarbeiter die Einwilligung nachweisen können, Art. 7 Abs. 1 i. V. m. ErwGr 42 DS-GVO.¹⁵

Die Voraussetzungen der Einwilligung sind nicht trennscharf voneinander abzugrenzen: So bedingt die Freiwilligkeit eine Informiertheit und diese wiederum setzt eine Fallbezogenheit voraus. Dennoch müssen die genannten Merkmale differenziert betrachtet werden, um „Stellschrauben“ herauszuarbeiten, die innovative, datenschutzrechtskonforme Einwilligungsmechanismen ermöglichen.

¹¹ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31–50.

¹² S. diesbezügl. EuGH, Urt. v. 01.10.2019, C-673/17, ECLI:EU:C:2019:801= GRUR 2019, 1198 Rn. 50, 60 ff. - Bundesverband/Planet49.

¹³ 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 Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final, 2017/0003 (COD).

¹⁴ S. auch EDPB (EDSA) Guidelines 5/2020, No. 11

¹⁵ Auf Einzelheiten wird hier nicht eingegangen, s. dazu EDPB (EDSA) Guidelines 5/2020, No. 104 ff.; Simitis/Hornung/Spiecker gen. Döhmman/Klement, Datenschutzrecht, 1. Aufl. 2019; Art. 7 Rn. 42 ff.; Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Auflage 2018, Art. 7 Rn. 22 f.

2.1.1.2. Form und unmissverständliche, eindeutige Einwilligung

2.1.1.2.1. Grundsatz: formfreie Einwilligung

Die Erteilung der Einwilligung ist grundsätzlich formfrei möglich, weshalb alle Willensbetätigungen mit Erklärungswert für die Willensbekundung ausreichen. Sie kann daher in jeder Form erfolgen, sei es schriftlich, elektronisch, mündlich oder konkludent.¹⁶ Die seitens der DS-GVO geforderte „Eindeutigkeit“ der Willensbekundung schließt konkludente Handlungen nicht aus, soweit das schlüssige Handeln unzweifelhaft eine Willensbekundung darstellt.¹⁷ Nur in Ausnahmefällen erfordert die DS-GVO eine ausdrückliche Einwilligung, insbesondere für die Verarbeitung sensibler Daten gem. Art. 9 Abs. 2 lit. a DS-GVO.¹⁸

Die Einwilligung muss auf jeden Fall unmissverständlich durch eine Erklärung oder sonstige „eindeutig bestätigende Handlung“ abgegeben werden.¹⁹ Hierzu ist eine „bewusste Handlung zur Einwilligung in die bestimmte Verarbeitung“ notwendig.²⁰ Nach ErwGr 32 DS-GVO kann bloßem Schweigen kein hinreichender Erklärungswert beigemessen werden. Ebenso wenig kann eine Einwilligung im Zuge reiner Untätigkeit des Datensubjekts oder mittels bereits (vor-)angeklickter Felder eingeholt werden, durch deren Deaktivierung der Betroffene seine Ablehnung demonstrieren muss um eine Einwilligungserteilung aktiv zu verhindern (sog. Opt-Out).²¹ Dies hat jüngst auch, der Ansicht des Generalanwalts Szpunar folgend,²² der Europäische Gerichtshof (EuGH) für die Verwendung von Werbe-Cookies festgestellt.²³ Die vormalige Praxis, Werbe-Cookies durch Opt-Out-Einwilligungen auf Basis des § 15 Abs. 3 TMG (als Umsetzung des Art. 5 Abs. 3 e-Privacy-RL) zu legitimieren, ist daher nicht länger zulässig.²⁴ Die frühere Rechtsprechung des Bundesgerichtshofs (BGH),²⁵ wonach ein Hinweis auf Vertragsklauseln mit fiktiv erteilten Erklärungen und das Nichtdurchstreichen einer vorformulierten Einwilligung in AGBs genügte, ist nach zutreffender Auffassung der Aufsichtsbehörden damit hinfällig.²⁶ Der BGH hat dies nunmehr in der Planet 49-Entscheidung ausdrücklich bestätigt, dass vorangekreuzte Einwilligungen bei

¹⁶ Simitis/Hornung/Spiecker gen. Döhmman/Klement, Datenschutzrecht, 1. Aufl. 2019; Art. 7 Rn. 39, Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 4 Rn. 24f; Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl. 2018 Art. 7 Rn. 35, 45.

¹⁷ Sydow/Ingold, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018; DS-GVO Art. 7 Rn. 23; Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 42; Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 37; Krohm ZD 2016, 368 (371); siehe zudem unten, 2.1.1.6.

¹⁸ Siehe unten, 2.1.1.2.2

¹⁹ Simitis/Hornung/Spiecker gen. Döhmman/Klement, DS-GVO, 1. Aufl. 2019, Art. 7 Rn 35.

²⁰ EDPB (EDSA) Guidelines 5/2020, No. 77.

²¹ Information Commissioner's Office, „Consent“, vers. 1.0.57, S. 30, 40; Ehmann/Selmayr/Heckmann/Peschke, DS-GVO Art. 7 Rn. 36, Schantz NJW 2016, 1841 (1844).

²² Schlussanträge des Generalanwalts M. Szpunar vom 21. März 2019 (Rn. 88 ff.), ECLI:EU:C:2019:246. Rechtssache C-673/17 Planet49 GmbH gegen Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.; s. auch den dazu gehörigen Vorlagebeschluss des BGH vom 05.10.2017 – I ZR 7/16.

²³ EuGH, Urt. v. 01.10.2019, C-673/17, ECLI:EU:C:2019:801= GRUR 2019, 1198 Rn. 57, 60 - Bundesverband/Planet49.

²⁴ Eine Übersicht über die bisherige Auslegungspraxis in Rauer/Ettig ZD 2018, 255 (256).

²⁵ BGH, Urt. v. 16.07.2008, VIII ZR 348/06; BGH, Urt. v. 11.11.2009, VIII ZR 12/08, s. auch BGH, Beschl. v. 05.10.2017 – I ZR 7/16, Rn. 25, 30.

²⁶ EDPB (EDSA) Guidelines 5/2020, No. 81; keine Einwilligung durch Akzeptanz von Allgemeinen Geschäftsbedingungen mit derselben Handlung; DSK Kurzpapier Nr. 20.

Cookies nicht den Anforderungen von Art. 4 Nr. 11 DS-GVO genügen und § 15 Abs. 3 TMG insoweit richtlinienkonform auszulegen ist.²⁷

Konkretere Vorgaben über die Art und Weise der Einwilligungseinholung trifft die DS-GVO nicht, weshalb verschiedenste Methoden und technische Umsetzungen gewählt werden können, etwa „Tickboxes“ oder „Einwilligungs-E-Mails“, solange ein eindeutiges Opt-In vorliegt.²⁸

Je nach Verarbeitungskontext bieten sich unterschiedliche Erteilungsformen an: Schriftliche Einwilligungen sind in „analogen“ Verarbeitungssituationen ratsam, in denen die Dokumentation der Einwilligungserteilung von besonderer Bedeutung ist.²⁹ Die Möglichkeit elektronisch abgegebener Einwilligungen, z.B. durch Anklicken eines Feldes, bietet sich insbesondere für die Legitimation von Datenverarbeitungen seitens digitaler Dienstleister an, da eine Einholung dieser Einwilligungsform im unmittelbaren Zusammenhang mit der Leistungserbringung erfolgen kann, z.B. indem ein Cookie-Banner oder Pop-Up-Fenster bei dem Besuch einer Website erscheint, mit der Möglichkeit, bestimmte Optionen anzuklicken.³⁰

2.1.1.2.2. Sonderfall: die ausdrückliche Einwilligung

In bestimmten Situationen bzw. soweit bestimmte Daten(-kategorien) verarbeitet werden sollen, verlangt die DS-GVO mit der „ausdrücklichen Einwilligung“ eine gesteigerte Form. Art. 9 Abs. 2 lit. a DS-GVO sieht die ausdrückliche Einwilligung für die Verarbeitung besonders sensibler Daten vor,³¹ ferner Art. 49 Abs. 1 lit. a DS-GVO für die Übermittlung an ein Drittland oder eine internationale Organisation (ohne angemessenen Datenschutz) oder Art. 22 Abs. 2 lit. c DS-GVO für automatisierte Entscheidungen einschließlich des Profilings.³²

Das Erfordernis einer ausdrücklichen Einwilligung erlangt insbesondere im Zusammenhang mit Gesundheitsdaten besondere Relevanz,³³ z.B. das Speichern von Patientendaten in der Cloud und die Verarbeitung entsprechender Daten aus Fitness- und Gesundheits-Apps, die von elektronischen Geräten wie

²⁷ BGH Urt. v. 28. Mai 2020 - I ZR 7/16 - Cookie-Einwilligung II

²⁸ S. auch Information Commissioner's Office, „Consent“, vers. 1.0.57, S. 40; Simitis/Hornung/Spiecker gen. Döhmnn/Klement, DS-GVO, 1. Aufl. 2019, Art. 7 Rn. 36; Buchner WRP 2018, 1283 (1285).

²⁹ Ein Ausgestaltungsvorschlag für eine schriftliche Patienteneinwilligung in: Otto/Rüdlin ZD 2017, 519 (524).

³⁰ Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 47.

³¹ Dies umfasst gem. Art. 9 Abs. 1 DS-GVO Daten über die „rassische“ und ethnische Herkunft, über politische, religiöse oder weltanschauliche Überzeugungen, über die Gewerkschaftszugehörigkeit sowie genetische und biometrische Daten, Gesundheitsdaten oder Daten über Sexualleben oder der sexuellen Orientierung.

³² Hierzu: WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251); Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 2; Gausling ZD 2019, 335 (338); Drewes ZD 2019, 296 (298); Galetzka DSRITB 2018, 45 (51).

³³ Kühnl/Rohrer/Schneider DuD 2018, 735 (738).

Wearables und Smart Watches erfasst werden.³⁴ Daneben ist auch an die Erbringung von Gesundheitsleistungen durch mobile Kommunikationsgeräte (sog. „Mobile-Health“) zu denken.³⁵

Bei der Bestimmung der besonderen Anforderungen an eine ausdrückliche Einwilligung ist zu beachten, dass es schon im Rahmen der „allgemeinen“ Einwilligung gem. Art. 7 DS-GVO einer eindeutig bestätigenden Handlung des Betroffenen bedarf, sodass Untätigkeit und Schweigen nicht zur wirksamen Erteilung genügen.³⁶ In Einklang mit dem sog. risikobasierten Ansatz des europäischen Datenschutzrechts, der im Kern besagt, dass mit zunehmender Eingriffsintensität der Verarbeitung auch die Anforderungen an die Rechtfertigung und Sicherheit der Verarbeitung steigen,³⁷ hebt das Ausdrücklichkeitserfordernis die Legitimationswirkung der Einwilligung an. Die geforderte „Ausdrücklichkeit“ verstärkt nicht zuletzt die Warnfunktion der Einwilligung.³⁸

Unabhängig von Nachweis- und Beweisgründen, ist das Merkmal der Ausdrücklichkeit dennoch nicht mit einem Schriftformerfordernis gleichzusetzen.³⁹

Nach Ansicht des (aus der Art.-29-Datenschutzgruppe hervorgegangenen) Europäischen Datenschutzausschusses (EDSA), kann ein gesondertes Feld, das auf einer Website mit „Ja“ oder „Nein“ angeklickt werden kann, genügen, sofern die Einwilligung deutlich hervorgehoben wurde.⁴⁰ Soweit eine angemessene Informiertheit und die Freiwilligkeit der Erteilung gewährleistet sind, soll demnach die Erklärung „*Hiermit willige ich in die Verarbeitung meiner Daten ein*“ genügen, nicht ausreichend wäre hingegen die Aussage „*Es ist klar, dass meine Daten verarbeitet werden*“.⁴¹ Die konkrete Formulierung sollte mithin hervorheben, dass der Betroffene (freiwillig) eine rechtserhebliche Wahl trifft, ob und wie seine Daten verarbeitet werden.

Die von EDSA entwickelten Anforderungen sind von vornherein auch mit der Sicherstellung einer angemessenen Dokumentation verknüpft. So würde nach Auffassung des EDSA ein

³⁴ Gola/Schulz DS-GVO, Art. 9 Rn 18; Werry/Knoblich MPR 2017, 1 (9); zur „Patienteneinwilligung“: Otto/Rüdling ZD 2017, 519.

³⁵ Grünbuch der EU-Kommission vom 10.04.2014 über Mobile-Health-Dienste, S. 8 ff., COM (2014) 219 final, SWD (2014) 135 final; Ehmann/Selmayr/Schiff, DS-GVO, 2. Aufl. 2018, Art. 9 Rn. 29; Gassner MPR 2015, 73 (79 ff.); Ortner/Daubenbüchel NJW 2016, 2918; Wolf GuP 2018, 129 (130 ff.); Dregelies VuR 2017, 256.

³⁶ Für weitere Ausführungen zur Bestätigungshandlung, s. 1.1.1.6.

³⁷ Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 9 Rn. 1; speziell zum risikobasierten Ansatz, s. Ehmann/Selmayr/Heberlein, DS-GVO, 2. Aufl. 2018, Art. 5 Rn 30; Veil ZD 2015, 347.

³⁸ Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 9 Rn. 7; Simitis/Hornung/Spiecker gen. Döhmman/Petri, Datenschutzrecht, 1. Aufl. 2019; Art. 9 Rn. 33; nach Ehmann/Selmayr/Schiff, DS-GVO, 2. Aufl. 2018, Art. 9 Rn 35 genügt die mündliche Erteilung hingegen nicht; zur Warnfunktion der Einwilligung, s. Krohm ZD 2016, 368 (371).

³⁹ Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 9 Rn 17; Ehmann/Selmayr/Schiff, DS-GVO, 2. Aufl. 2018, Art. 9 Rn 30; Tinnefeld/Conrad ZD 2018, 391 (395).

⁴⁰ EDPB (EDSA) Guidelines 5/2020, No. 96. hier böte sich, ähnlich wie im Rahmen von AGB eine deutliche Hervorhebung, z.B. durch Fettschrift oder eine Umrandung an, EuGH, Ur. v. 01.10.2019, C-673/17, ECLI:EU:C:2019:801= GRUR 2019, 1198 Rn. 58 ff. - Bundesverband/Planet49; LG München I, Ur. v. 11.10.2018 – 12 O 19277/17, BeckRS 2018, 31023 Rn. 44;

⁴¹ EDPB (EDSA) Guidelines 5/2020, No. 96

„offensichtlicher Weg zum Einholen einer ausdrücklichen Einwilligung [...] [sein], dass die Einwilligung in einer schriftlichen Erklärung ausdrücklich bestätigt wird. Der Verantwortliche könnte gegebenenfalls sicherstellen, dass die Erklärung von der betroffenen Person unterzeichnet wird, um alle möglichen Zweifel und einen möglicherweise fehlenden Nachweis für die Zukunft aus dem Weg zu räumen.“⁴²

Der EDSA übersieht dabei auch nicht, dass ein solcher schriftformbasierter Einwilligungsmechanismus Probleme aufwerfen kann, insbesondere im digitalen bzw. Online-Kontext, zumal die DS-GVO keine expliziten Formalitäten vorschreibt. Dem Ausdrücklichkeitserfordernis würde aus Sicht des EDSA im Rahmen von IT-Diensten daher auch entsprochen, wenn

„[...] eine betroffene Person die erforderliche Erklärung durch Ausfüllen eines elektronischen Formulars, Senden einer E-Mail, Hochladen eines eingescannten Dokuments, das von der betroffenen Person unterzeichnet wurde oder durch Verwenden einer elektronischen Signatur erteilen [kann].“⁴³

Um im digitalen Kontext eine mit der Schriftform vergleichbare Schutzwirkung zu erreichen, empfiehlt der EDSA jedoch ein „doppeltes Verfahren“ (auch „Double-Opt-In“ genannt), indem die betroffene Person nochmals ausdrücklich per Hyperlink oder SMS-Code die Einwilligung bestätigt.⁴⁴ Ähnliche Verifizierungsmechanismen werden ferner im Rahmen der Einwilligung Minderjähriger diskutiert.⁴⁵

2.1.1.3. Bezogen auf einen bestimmten Fall

Die Einwilligung muss stets für einen bestimmten Zweck und bezogen auf konkrete Datenverarbeitungsvorgänge erteilt werden.⁴⁶ Der EDSA leitet zu Recht aus ErwGr 32 DS-GVO her, dass die Einwilligung bei einer Verarbeitung zu mehreren Zwecken stets gesondert für jeden Zweck zu erteilen ist (sog. „Granularität“); andernfalls fehlt es der Einwilligung an der Freiwilligkeit.⁴⁷ Gleiches gilt, wenn der Verantwortliche die Durchführung mehrerer (zweckgleicher) Verarbeitungsprozesse beabsichtigt, auch dann muss die Einwilligung sich auf jeden dieser Prozesse beziehen.⁴⁸

Es empfiehlt sich daher die Verwendung sog. „differenzierter Einwilligungen“, bei denen der Betroffene in einzelne Zwecke und Verarbeitungen voneinander losgelöst einwilligen kann – die Nutzung von Global-/ und Generaleinwilligungen

⁴² EDPB (EDSA) Guidelines 5/2020, No. 93

⁴³ EDPB (EDSA) Guidelines 5/2020, No. 94

⁴⁴ EDPB (EDSA) Guidelines 5/2020, No. 98; Ehmman/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl. 2018, Art. 7 Rn 70; ähnliche Verfahren haben sich bereits im Wettbewerbsrecht etabliert, s. Fezer/Büschler/Obergfell/Mankowski, Lauterkeitsrecht: UWG, 3. Aufl. 2016, § 7 Rn. 219 ff.

⁴⁵ Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 8 Rn. 10, 13; Paal/Pauly/Frenzel, DS-GVO, 2. Aufl. 2018, Art. 8 Rn 13; Möhrke-Sobolewski/Klas K&R 2016, 373 (377 f.).

⁴⁶ Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 7, Art. 7 Rn 61; Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 34 ff.; Sydow/Ingold, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018; DS-GVO Art. 7 Rn. 38 ff.

⁴⁷ EDPB (EDSA) Guidelines 5/2020, No. 42 ff. 14.

⁴⁸ S. ErwGr 43 S. 2; Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 4 Rn. 26.

ist nicht länger statthaft.⁴⁹ Das Gebot der Fallbezogenheit schließt daher Pauschaleinwilligungen aus, also die Einwilligung in alle beliebigen Zwecke für den Verarbeiter, nicht aber „standardisierte“ Einwilligungen.⁵⁰ Standardisiert meint hier, dass in einen eher generalisierten Zweck der Verarbeitung eingewilligt wird (z.B. E-Mail zur Werbung durch den Verarbeiter) und in der Folge jede Handlung zu diesem Zweck von der Einwilligung umfasst ist (also nicht jede neue E-Mail einer gesonderten Einwilligung bedarf). Wenn also zum Zeitpunkt der Datenerhebung differenziert und situationsabhängig darüber aufgeklärt wird, auf welche konkreten Zwecke und Mittel (und seitens welcher Verantwortlichen und Auftragsverarbeiter) sich die Einwilligung erstreckt, so kann sich die Einwilligung bis zu ihrem Widerruf auch auf weit in der Zukunft liegende, sachgleiche Verarbeitungen beziehen.

Dazu ein Beispiel: Zulässig ist, dass ein Webshop-Betreiber „A“ die Nutzerinnen und Nutzer seiner Plattform darüber informiert und jeweils differenziert zu einer Einwilligungserteilung auffordert, dass erstens die bereitgestellten (E-Mail-) Adressdaten zukünftig zu Zwecken der direkten werblichen Ansprache durch „A“ gespeichert und genutzt werden [„Einwilligungsfeld 1“] und zweitens eine Weitergabe dieser Daten an Webshop „B“ erfolgt, der die Daten seinerseits speichert und zur werblichen Ansprache nutzt [„Einwilligungsfeld 2“].

Die Granularität bzw. Differenziertheit hinsichtlich der Zwecke und Verarbeitungsvorgänge bei der Einwilligung dient dazu, den Betroffenen vor Einwilligungen in Verarbeitungskomplexe zu schützen, deren Ablauf und Reichweite er nicht überblicken kann.⁵¹ Sie sollte jedoch nicht dahingehend missinterpretiert werden, dass von dem Verantwortlichen Datenverarbeitungen künstlich in verschiedene Teilprozesse aufgespalten werden, in die, obwohl notwendig miteinander verknüpft, separat eingewilligt werden muss.⁵² So ist zur Auswertung des Fitnesszustands eines Betroffenen die Erhebung und (Zwischen-)Speicherung personenbezogener Daten notwendig, sodass eine einzige Einwilligung zum „Zweck der Zustandsauswertung“ alle drei Teilprozesse (Erhebung, Speicherung, Analyse) der Verarbeitung umfassen kann. Aus Transparenzgründen ist dennoch eine Information von Nutzerinnen und Nutzern über den genauen Ablauf des Gesamtprozesses (inkl. inbegriffener Teilprozesse) erforderlich. Für die Nutzung der Daten zu Zwecken des Direktmarketings oder der Weitergabe an Dritte, müsste die Einwilligung jedoch zweifellos separate „Tick-Boxes“ o.ä. bereithalten (s. zuvor benanntes Beispiel). Für vergleichbare Fälle hat der EuGH in der „Planet-49-Entscheidung“ hervorgehoben, dass die Einwilligung in die Verarbeitung personenbezogener Daten zur Durchführung eines Gewinnspiels nicht die Einwilligung in die Speicherung von Cookies mitumfasst.⁵³

⁴⁹ Ebenso Schantz/Wolff/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, D. Rn. 517 f.; Buchner DuD 2015, 155 (158).

⁵⁰ Specht/Mantz/Sassenberg, Handbuch Europäisches und deutsches Datenschutzrecht 1. Aufl. 2019, § 28 Rn. 39.

⁵¹ Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 63; Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 61; Schantz, NJW 2016, 1841 (1844).

⁵² Ähnl. Simitis/Hornung/Spiecker gen. Döhmann/Klement, Datenschutzrecht 1. Aufl. 2019, Art. 7 Rn. 6.

⁵³ EuGH, Urt. v. 01.10.2019, C-673/17, ECLI:EU:C:2019:801= GRUR 2019, 1198 Rn. 59 ff. - Bundesverband/Planet49.

2.1.1.4. In Kenntnis der Sachlage (Informed consent)

Neben der Freiwilligkeit⁵⁴ muss die Einwilligung auf der Grundlage angemessener Informationen erfolgen („informed consent“). Der Europäische Datenschutzausschuss verlangt in diesem Zusammenhang einen bestimmten Katalog an Mindestinformationen:

- „(i) die Identität des Verantwortlichen
- (ii) der Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird
- (iii) die (Art) Daten, die erhoben und verwendet werden
- (iv) das Vorliegen des Rechts, die Einwilligung zu widerrufen,
- (v) gegebenenfalls Informationen über die Verwendung der Daten für eine automatisierte Entscheidungsfindung gemäß Artikel 22 Absatz 2 Buchstabe c, und
- (vi) Angaben zu möglichen Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien gemäß Artikel 46.“⁵⁵

Im Rahmen der „Planet-49-Entscheidung“ konkretisierte der EuGH, dass zur informierten Einwilligung des Betroffenen in die Verwendung von Werbe-Cookies auch Angaben zur Funktionsdauer der Cookies und der Zugriffsmöglichkeit Dritter bereitgestellt werden müssen.⁵⁶ Zudem hob der EuGH in der „Fashion-ID-Entscheidung“ hervor, dass der Betreiber einer Website zur Einholung einer Einwilligung über die Nutzung von sog. „Social Plugins“ verpflichtet ist, die den Browser des Betroffenen veranlassen, Nutzerdaten an den Plugin-Anbieter zu übersenden und Inhalte von diesem zu beziehen, soweit der Betreiber als Joint-Controller mit dem Plugin-Anbieter (hier facebook) auftritt - eine spätere Einwilligungseinholung und Information seitens des Plugin-Anbieters (ebenfalls als Joint-Controller) bietet demnach keinen hinreichenden Schutz des Betroffenen.⁵⁷

Wie diese Informiertheit des Datensubjekts konkret erreicht werden soll, schreibt die DS-GVO nicht vor. Allerdings betonen die Aufsichtsbehörden zu Recht die Notwendigkeit einer klaren und einfachen, unmissverständlichen Sprache, auch unter Berücksichtigung der jeweiligen Zielgruppe, insbesondere bei schriftlichen oder vergleichbaren digitalen Einwilligungsaufforderungen.⁵⁸

Nach ErwGr 42 S. 3 u. 4 DS-GVO kann auf ein vorformuliertes Einwilligungsersuchen zurückgegriffen werden, soweit es in verständlicher, leicht zugänglicher

⁵⁴ S. dazu 2.1.1.5.

⁵⁵ EDPB (EDSA) Guidelines 5/2020, No. 64.

⁵⁶ EuGH, Urt. v. 01.10.2019, C-673/17, ECLI:EU:C:2019:801= GRUR 2019, 1198 Rn. 59 ff. - Bundesverband/Planet49.

⁵⁷ EuGH, Urt. v. 29.07.2019, C-40/17, ECLI:EU:C:2019:629 = GRUR 2019, 977 Rn. 101 ff. - Fashion ID; ob der EuGH in der Einwilligung den einzig möglichen Rechtfertigungsgrund für derartige Plugins erblickt, wird jedoch nicht deutlich, hierzu auch *Kremer* CR 2019, 676 (679).

⁵⁸ A EDPB (EDSA) Guidelines 5/2020, No. 67 ff.; Kühling/Buchner/*Buchner/Kühling*, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 60; *Ernst*, ZD 2017, 110 (113); zum Umfang der Informationspflichten bei Verwendung von digitalen Assistenten s. *Gausling*, ZD 2019, 335 (337).

Form (z.B. einer klaren und einfachen Sprache) verfasst ist, keine missbräuchlichen Klauseln enthält und den Betroffenen als Mindestanforderung darüber in Kenntnis setzt, wer Verantwortlicher ist und welche Zwecke die Datenverarbeitung verfolgt.⁵⁹ Trotz des Verweises des ErwGr 42 S. 3 auf die Richtlinie 93/13/EWG⁶⁰, sieht der verfügende Teil der DS-GVO keine unmittelbare Missbrauchskontrolle im Sinne der Richtlinie 93/13/EWG vor.⁶¹ Dennoch bleibt eine Angemessenheitskontrolle des in den AGB formulierten Einwilligungensuchens nach Maßgabe der nationalen Vorschriften, hier § 307 Abs. 1 S. 1 BGB, möglich.⁶² Insbesondere das Transparenzgebot in § 307 Abs. 1 S. 1 BGB kann hier fruchtbar gemacht werden, überschneidet sich aber mit den schon unter Art. 7 Abs. 4 DS-GVO entwickelten Maßstäben, dass für eine wirksame Einwilligung allgemein verständliche, klare Angaben hinsichtlich der Datenverarbeitung erforderlich sind. Das Transparenzgebot kann auch nicht dadurch zu Gunsten des Verarbeiters gelockert werden, indem Nutzerinnen und Nutzer in AGB erklären, sie haben die Datenschutzbestimmungen gelesen und verstanden. Eine solche Klausel wäre als Tatsachenbestätigung nach §§ 307, 309 Nr. 12 b) BGB unwirksam.⁶³ Auch eine Inhaltskontrolle der Einwilligung ist denkbar, auch wenn diese neben den Vorschriften der DS-GVO wenig eigenes Gewicht haben wird, weil regelmäßig anhand des gesetzlichen Leitbilds, hier der DS-GVO, zu entscheiden ist.⁶⁴

Formulärmäßige Einwilligungensuche müssen zudem deutlich abgehoben von anderen Vertragsbedingungen erfolgen; denkbar sind die Bereitstellung in einem eigenen Dokument oder getrennten Bildschirm sowie die visuelle Abgrenzung durch Rahmen, Kästen oder Fettschrift, etc.⁶⁵ Die Informiertheit des Betroffenen darf mithin nicht dadurch beeinträchtigt werden, dass der konkrete Einwilligungsinhalt durch wenig sachdienliche Ausführungen verschleiert wird, oder dass die datenschutzrechtliche Einwilligung (z.B. als Annex von AGB) gar nicht erst als solche identifiziert wird.⁶⁶

ErwGr 32 S. 6 hebt hervor, dass insbesondere elektronische Einwilligungsaufforderungen von (Online-)Diensten klar und knapp gefasst sein sollten, um die

⁵⁹ So auch DSK Kurzpapier Nr. 20; s. auch Kühling/Buchner/*Buchner/Kühling*, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 59; Ehmman/Selmayr/*Heckmann/Pascke*, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 40 ff.; Sydow/*In-gold*, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 34 ff.

⁶⁰ Richtlinie 93/13/EWG des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen, ABi. L 95 vom 21.04.1993, S. 29.

⁶¹ Simitis/Hornung/Spiecker gen. Döhmman/*Klement*, Datenschutzrecht, 1. Aufl. 2019; Art. 7 Rn. 80.

⁶² Simitis/Hornung/Spiecker gen. Döhmman/*Klement*, Datenschutzrecht, 1. Aufl. 2019; Art. 7 Rn. 81; differenzierend *Wendehorst/v. Westphalen* NJW 2016, 3745 (3748).

⁶³ BGH, Beschl. v. 28.03.1996 - III ZR 95/95; LG Berlin, Urt. v. 16.01.2018 – 16 O 341/15 Rn. 60;

⁶⁴ Vgl. noch zur DSRL BGH, Urt. v. 11.11.2009 - VIII ZR 12/08, NJW 2010, 864 – Happy Digits, der aber dann nicht die Einwilligung der Inhaltskontrolle unterwerfen will, wenn sie die gesetzlichen Vorgaben erfüllt; BGH, Urteil vom 25.10.2012 – I ZR 169/10, NJW 2013, 2683 Rn. 22f; BGH, Urteil vom 16.07.2008 - VIII ZR 348/06; wie hier auch Simitis/Hornung/Spiecker gen. Döhmman/*Klement*, Datenschutzrecht, 1. Aufl. 2019; Art. 7 Rn. 81; zur vergleichbaren Lage unter der DSRL *Nord/Manzel*, NJW 2010, 3756.

⁶⁵ EDPB (EDSA) Guidelines 5/2020, No. 71, insbesondere für kleine Bildschirme; Simitis/Hornung/Spiecker gen. Döhmman/*Klement*, Datenschutzrecht, 1. Aufl. 2019, Art. 7 Rn. 73; *Tinnefeld/Conrad*, ZD 2018, 391 (394); *Ernst* ZD 2017, 110 (113).

⁶⁶ Spindler/Schuster/*Spindler/Dalby*, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 7 Rn. 9; *Ernst*, ZD 2017, 110 (113).

digitalen Inhalte nicht unnötig zu unterbrechen. Wie eine „unnötige Unterbrechung“ zu bestimmen ist, ist allerdings unklar.⁶⁷ Die Nutzung von Cookie-Bannern und Pop-up-Fenstern,⁶⁸ die den gesamten Bildschirm einnehmen und den eigentlichen Inhalt (z.B. durch „Ausgrauung“) unkenntlich machen oder die wiederholt erfolgen, verhindern einen ungehinderten Zugang zum angebotenen Dienst. Da die Einwilligungsaufforderung auch unter minimaler Dienst einschränkung erfolgen könnte, etwa mittels einer dezenten Einblendung am Bildschirmrand, kollidieren ganzseitige Einblendungen und Popups mit dem Gebot aus ErwGr 32 S. 6 und sollten unterlassen werden.⁶⁹

Schließlich ergibt sich eine erhebliche Überschneidung mit den allgemeinen Informationspflichten nach Art. 12 i. V. m. 13, 14 DS-GVO, welche unabhängig vom Rechtfertigungsgrund eingreifen, die aber bereits auf den ersten Blick die erhebliche Schnittmenge mit den für die Informiertheit des Einwilligenden erforderlichen Angaben zeigt:⁷⁰ So muss nach Art. 13 Abs. 1 lit. a DS-GVO die Identität des Verantwortlichen, nach lit. c die Datenverarbeitungszwecke (also für die Einwilligung die Fallbezogenheit) sowie lit. e die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten genannt werden. Auch über die Widerrufsrechte bei der Einwilligung muss vorab informiert werden, Art. 13 Abs. 2 lit. c DS-GVO. Des Weiteren ist gemäß Art. 13 Abs. 2 lit. f DS-GVO hinsichtlich der automatischen Verarbeitung nach Art 22 DS-GVO und gemäß Art. 13 Abs. 1 lit. f DS-GVO über die Risiken von Datenübermittlungen ohne Angemessenheitsbeschluss zu informieren. Die Informationen, die der EDSA für eine informierte Einwilligung für notwendig hält,⁷¹ finden sich also alle, bis auf Informationen zur Art der Daten, in Art. 13 DS-GVO wieder. Das bedeutet aber nicht, dass deshalb die Informiertheit der Einwilligung inhaltsgleich mit den Informationspflichten nach Art. 13 DS-GVO wäre. Dem Wortlaut des Art. 13 DS-GVO nach ist klar, dass dieser erst zu einem späteren Zeitpunkt eingreift („zum Zeitpunkt der Erhebung“), wohingegen die Informationen zur Einwilligung denknötwendig vor der Erteilung der Einwilligung vorliegen müssen. Zudem setzt Art. 13 DS-GVO bereits eine vorhandene Rechtsgrundlage voraus, vgl. Art. 13 Abs. 1 lit. c DS-GVO. Auch der zuvor genannte ErwGr 32 S. 6 lässt darauf schließen, dass es bei der Informiertheit bei der Einwilligung nicht auf einen umfassenden Katalog von Informationspflichten ankommen kann, da ansonsten die Aufforderung nicht mehr knapp zu fassen wäre. Auch der EDSA stellt explizit klar, dass die Informationen für die Einwilligung nicht mit den Informationen nach Art. 13 DS-GVO deckungsgleich sind.⁷² Demgemäß muss genau differenziert werden, zu

⁶⁷ Forgó/Helfrich/Schneider/Arning/Born, *Betrieblicher Datenschutz*, 3. Aufl. 2019, Kapitel 2 Rn. 63.

⁶⁸ Spezielle hierzu *Rauer/Ettig ZD* 2015, 255 (257).

⁶⁹ Ähnl. *Härtig*, *Datenschutz-Grundverordnung*, 1. Aufl. 2016, Rn. 363; *Gola/Schulz*, *DS-GVO*, 2. Aufl. 2018, Art. 7 Rn. 47.

⁷⁰ *Ehmann/Selmayr/Heckmann/Paschke*, *DS-GVO*, 2. Aufl., Art. 12 Rn. 6 f;

⁷¹ S. oben 2.1.1.4.

⁷² EDPB (EDSA) Guidelines 5/2020, No. 72, 170..

welchem Zeitpunkt eingewilligt und zu welchem Zeitpunkt⁷³ Daten erhoben werden. Davon abhängig sind die einzuhaltenden Informations- und Transparenzpflichten.⁷⁴

Zudem kann nach Art. 13 Abs. 4 DS-GVO auf die danach notwendigen Informationen verzichtet werden, wenn der Betroffene bereits über die entsprechenden Informationen verfügt, sodass theoretisch auf eine Wiederholung einiger Informationen verzichtet werden kann, wenn vor der Datenerhebung im Rahmen der Einwilligung informiert wurde. Faktisch wird aber in den allermeisten Fällen, insbesondere im Online-Bereich, immer schon eine Datenverarbeitung in Form der Speicherung von IP-Adressen vorliegen, die einer Erteilung der Einwilligung zeitlich vorgeht.⁷⁵ Eine Belehrung vor dem eigentlichen Aufrufen der Website kann jedoch nicht erwartet werden, wie auch ErwGr 58 S. 2 zeigt, der explizit die Möglichkeit der Belehrung auf der Website nennt. Für den Verkehr im Internet hat das zur Folge, dass jedenfalls immer die Informationspflichten nach Art. 13, 14 DS-GVO unmittelbar nach Aufruf einer Seite zu erfüllen sind. Parallel sind die Fälle zu behandeln, in denen die Übermittlung der Daten von Seiten des Dateninhabers erfolgen, z.B. bei Initiativ-Bewerbungen oder Anfragen ohne vorherigen Kontakt.⁷⁶

2.1.1.5. Freiwilligkeit und Koppelungsverbot

Aufgrund des Charakters der Einwilligung als unmittelbarer Ausdruck der informationellen Selbstbestimmung legt die DS-GVO (und die Aufsichtsbehörden) großes Gewicht auf die Freiwilligkeit der Einwilligungserteilung. Nach ErwGr 42 S. 5 DS-GVO muss der Betroffene eine echte und freie Wahl haben, um eine wirksame Einwilligung zu erteilen, Nachteile dürfen der betroffenen Person durch die Nichterteilung oder den Widerruf der Einwilligung nicht entstehen. Die Einwilligung muss sich daher grundsätzlich als „verhandelbar“ darstellen.⁷⁷ Dies hatte nach Auffassung der britischen Datenschutzaufsicht indes nicht ausgeschlossen, dass die Einwilligung mit Anreizen versehen wird, z.B. indem zusätzliche Dienste bzw. ein größerer Funktionsumfang angeboten werden.⁷⁸

Ob die DS-GVO ein echtes Verbot der Koppelung eines Vertragsabschlusses mit der Einwilligung zur Verarbeitung von Daten enthält, die nicht zur Erfüllung eines Vertrages (dann wäre Art. 6 Abs. 1 b) einschlägig) benötigt werden, ist umstritten.⁷⁹ Die Aufsichtsbehörden gehen hiervon aufgrund Art. 7 Abs. 4 i. V.

⁷³ Zum Zeitpunkt für Informationen nach Art. 13 f s. Kühling/Buchner/Bäcker, DS-GVO, 2. Aufl. 2018, Art. 13 Rn. 56 ff; Spindler/Schuster/Nink, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 13 Rn. 20.

⁷⁴ Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl., Art. 12 Rn. 6 f; vgl. auch BeckOK Datenschutzrecht/Stemmer, DS-GVO, 30. Ed. 1.11.2019, Art. 7 Rn. 55; Simitis/Hornung/Spiecker gen. Döhmman/Klement, DS-GVO, 1. Aufl. 2019, Art. 7 Rn. 73; für eine Synchronisation von Art. 7 und Art.12 ff aber Sydow/Ingold, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 35.

⁷⁵ Spindler/Schuster/Nink, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 13 Rn. 20; vgl. auch Gola/Franck, DS-GVO, 2. Aufl. 2018, Art. 13 Rn. 36 f.

⁷⁶ Gola/Franck, DS-GVO, 2. Aufl. 2018, Art. 13 Rn. 36.

⁷⁷ EDPB (EDSA) Guidelines 5/2020, No. 13.

⁷⁸ Information Commissioner's Office, „Consent“, vers. 1.0.57, S. 28.

⁷⁹ S. zum Spannungsverhältnis von Art. 7 Abs. 4, 6 Abs. 1 b) und ErwGr 43, Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl., Art. 7 Rn. 94 ff.; Engeler ZD 2018, 55 (59); Härting ITRB 2017, 42 (43).

m. ErwGr 43 S. 2 DS-GVO aus⁸⁰ – auch wenn dieses Verbot nicht im verfügbaren Teil der DS-GVO enthalten ist. Demgemäß soll jede Einwilligung zur Verarbeitung von Daten, die nicht für die vertragliche Leistung erforderlich ist, die aber zur Bedingung für den Vertragsabschluss gemacht wird (sog. Kopplung), gegen Art. 7 Abs. 4 DS-GVO verstoßen. Ebenso wäre eine Einwilligung für verschiedene Datenverarbeitungszwecke, die allesamt miteinander gekoppelt werden und bei denen keine Differenzierung möglich ist (etwa indem der Betroffene für einen Verarbeitungsprozess keine Einwilligung erteilt, für einen anderen aber schon), unzulässig, da der Betroffene hier keine freie Wahl hat.⁸¹ Es liegt daher nahe, aus der DS-GVO auch in Bezug auf die Freiwilligkeit die Notwendigkeit einer sog. „differenzierten“ Einwilligung abzuleiten, also die Pflicht, jedem Verarbeitungszweck gesondert zustimmen zu können, ohne dass eine Verweigerung der Zustimmung Einfluss auf den Inhalt des Vertrags hätte.⁸² Insbesondere ErwGr 43 der DS-GVO legt diesen Schluss nahe, heißt es dort doch, dass die Einwilligung sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen sollte. Holt der Verarbeiter also die Einwilligung für mehrere Zwecke ein, ohne dem Betroffenen die Möglichkeit zu geben, gesondert in diese einzuwilligen, muss die Freiwilligkeit abgelehnt werden.

Viele Stimmen in der Literatur befürworten hingegen eher ein „unechtes“ Kopplungsverbot, wonach nicht jede Kopplung von Einwilligung und zweckfremder Verarbeitung verboten ist, sondern diesen Umständen lediglich in hohem Maße Rechnung getragen werden soll.⁸³ Auch nach dieser abweichenden Ansicht sind aber an die Freiwilligkeit strenge Anforderungen zu stellen, wenn der Verantwortliche den Vertragsschluss an eine Einwilligung des Betroffenen koppelt, die die Verarbeitung von vertraglich nicht erforderlicher Daten betrifft. Wie der österreichische OGH unlängst festgestellt hat, müsse der Verantwortliche in derartigen Fällen besondere Umstände vortragen, die die Freiwilligkeit der Einwilligung belegen.⁸⁴ Ähnlich äußerte sich jüngst auch das OLG Frankfurt/M., das ausführt, dass die Verknüpfung einer Einwilligung in eine Datenverarbeitung und einer damit nicht zusammenhängenden Glücksspielteilnahme nicht zur Unfreiwilligkeit der erteilten Einwilligung führe.⁸⁵ Ein strenges Kopplungsverbot würde auch das Geschäftsmodell „Leistung gegen Daten“, und damit gleichzeitig die Entscheidung des europäischen Gesetzgebers für eine solche Möglichkeit in Art.

⁸⁰ DSK Kurzpapier Nr. 20; *Buchner* WRP 2018, 1283 (1286).

⁸¹ Die hM sieht allerdings hier kein absolutes Verbot, sondern nur ein „Sollen“, da sich dies nur aus ErwGr 42 S. 2 und nicht dem verfügbaren Teil ableiten lässt, dazu auch unten.

⁸² *Ehmann/Selmayr/Heckmann/Paschke*, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 64; *Schantz*, NJW 2016, 1841 (1845); *Schantz/Wolff/Wolff*, DatenschutzR, 1. Aufl. 2017, Rn. 517; dazu auch bereits ausführlich bei 2.1.1.3.

⁸³ *Paal/Pauly/Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 18; *Engeler*, ZD 2018, 55 (59); *Härting*, ITRB 2017, 42 (43); *Hacker*, ZfPW 2019, 148 (182 f); *Metzger*, AcP 216 (2016), 818 824).

⁸⁴ OGH, Urteil vom 31. 8. 2018, – 6Ob140/18 h Ziff. 4.4.4, ZD 2019, 72 Rn. 46.

⁸⁵ OLG Frankfurt/M., Urt. v. 27.6.2019 – 6 U 6/19, ZD 2019, 507 Rn. 12 mit Anm. *Eckhardt et al.*

3 DI-RL⁸⁶, obsolet machen.⁸⁷ Auch der Wortlaut des Art. 7 Abs. 4 DS-GVO verbietet keine strenge Kopplung, sondern verlangt nur nach „Berücksichtigung“. Der intendierte Schutz von Verbraucherinnen und Verbrauchern vor sich selbst muss hier Berücksichtigung finden, aber auch dort seine Grenzen haben, wo erst nach der Abwägung aller Umstände und höchstmöglicher Transparenz eine Entscheidung getroffen wird; andernfalls würde man wiederum die informationelle Privatautonomie von Verbraucherinnen und Verbrauchern beschneiden.⁸⁸ Dies deckt sich auch mit dem erklärten Ziel der DS-GVO, die Persönlichkeitsrechte des Einzelnen zu schützen und gleichzeitig den digitalen Binnenmarkt zu stärken,⁸⁹ indem es dem Schutz von Datensubjekten umfassend Rechnung trägt und unter strengen Auflagen eine wirtschaftliche Nutzbarkeit ermöglicht. Weiteres starkes Indiz für eine Freiwilligkeit in solchen Fällen kann z.B. auch sein, dass der Dienstanbieter einen „kostenlosen“ Service gegen die Erteilung einer Einwilligung anbietet und eine kostenpflichtige Alternative vorhält, die im Falle der Einwilligungsverweigerung gewählt werden kann.⁹⁰ Allerdings hält der EDSA sog. Cookie-Walls explizit für unzulässig, da die Einwilligung nicht freiwillig erteilt werde. Cookie-Walls verhindern den Zugang zu Inhalten auf einer Webseite, wenn der Nutzer nicht der Setzung von Cookies zustimmt.⁹¹

Davon abzugrenzen, aber praktisch oft eng verbunden, sind Fälle, in denen die Verarbeitung personenbezogener Daten für die Leistungserbringung tatsächlich erforderlich ist⁹² oder der Verantwortliche dem Betroffenen die Erteilung der Einwilligung zu Disposition stellt, ohne daran positive oder negative Konsequenzen zu knüpfen.⁹³ Art. 6 Abs. 1 lit. b und Art. 7 Abs. 4 DS-GVO schließen sich folglich aus.⁹⁴ Nach Auffassung des EDSA ist der Begriff der „Erforderlichkeit“ für die Vertragserfüllung i. S. d. Art. 6 Abs. 1 lit. b eng im Sinne einer „Notwendigkeit“ auszulegen,⁹⁵ sodass zum Beispiel der Vertragsschluss (z.B. die Namensnennung bei Abschluss eines Mobilfunkvertrags) oder die Leistungserbringung (z.B. die Nennung der Adressdaten beim Online-Kauf) ohne die beabsichtigte Datenverarbeitung nicht erfolgen könnte.⁹⁶ Erleichtert die Datenverarbeitung lediglich

⁸⁶ Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABL. 136 S. 1.

⁸⁷ Ehmann/Selmayr/Heckmann/Heberlein, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 7.

⁸⁸ Schantz, NJW 2016, 1841, 1845; Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 95.

⁸⁹ Art. 1 Abs. 1 DS-GVO, ErwGr 4. S. 2.

⁹⁰ Zu diesem Modell Golland, MMR 2018, 130 (133 f).

⁹¹ EDPB (EDSA) Guidelines 5/2020, No. 40.

⁹² Der Europäische Datenschutzausschuss hebt diesbezüglich die konzeptuellen Unterschiede der Erlaubnistatbestände aus Art. 6 Abs. 1 lit. a und b DS-GVO hervor, s. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, S. 7.

⁹³ Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 7 Rn. 14 mwN.

⁹⁴ EDPB (EDSA) Guidelines 5/2020, No. 13 ff, 25 ff. mit dem Beispiel (No 15) einer App zur Bildbearbeitung, die gleichzeitig geolokale Daten und die Zustimmung zur verhaltensorientierten Werbung verlangt; s. auch Engeler ZD 2018, 55, 58, Golland MMR 2018, 130 (131) je mwNachw.

⁹⁵ EDPB (EDSA) Guidelines 5/2020, No. 32; weiterführend Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 6 Rn. 5f; Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 49 ff.

⁹⁶ Für weitere Beispiele s. Metzger GRUR 2019, 129 (132).

die Vertragserfüllung, die jedoch auch unter Einsatz anderer (ggf. aufwendigerer) Mittel realisierbar wäre, so ist nach Ansicht des EDSA eine Erforderlichkeit abzulehnen.⁹⁷ Auch die wirtschaftliche Notwendigkeit der Refinanzierung eines Geschäftsmodells rechtfertigt danach nicht die Monetarisierung von Daten im Zuge des Art. 6 Abs. 1 lit. b DS-GVO, da die Verwertung der Daten aus Sicht des Betroffenen weder für den Vertragsschluss noch für den Vertragszweck unabdingbar ist.⁹⁸ Ebenso wenig genügt es nach Ansicht des EDSA für die Freiwilligkeit, wenn der Verantwortliche auf alternative Anbieter verweist, die ohne zusätzliche Daten die gleichen Leistungen erbrächten und der Betroffene dennoch das Angebot des Verantwortlichen wahrnimmt.⁹⁹ Verneint wird die Erforderlichkeit also immer dann, wenn die Verarbeitung hinweggedacht werden könnte, ohne dass der Durchführungserfolg der Vertrags dadurch beeinträchtigt wird.¹⁰⁰ Geprüft werden muss immer auch, ob die Verarbeitung der Daten im Vergleich zu anderen Optionen zur Erreichung des Ziels, das am wenigsten „aufdringliche“ Mittel ist – es hat also gewissermaßen eine Erforderlichkeitsprüfung stattzufinden.¹⁰¹ Grund und Ausmaß der notwendigen Datenverarbeitung sind Verbraucherinnen und Verbrauchern in transparenter Weise offenzulegen.¹⁰² Eine Berufung auf den Art. 6 Abs. 1 lit. b DS-GVO soll darüber hinaus nur dann möglich sein, wenn der Vertrag auch tatsächlich rechtswirksam entstanden ist.¹⁰³ Seitens des EDSA werden also sehr enge Grenzen für eine Berufung auf das Notwendigkeitskriterium gezogen.

Vereinzelt wird hingegen mit Hinblick auf das im Internet weit verbreitete Geschäftsmodell „Leistung gegen Daten“ dafür plädiert, das Merkmal „zur Erfüllung ... notwendig“ i. S. d. Art. 6 Abs. 1 lit. b DS-GVO weit auszulegen, mit der Folge, dass das als notwendig gelte, was die Parteien als solches vereinbaren.¹⁰⁴ Andernfalls würden solche Verträge mit hoher Wahrscheinlichkeit am Kopplungsverbot scheitern. Für diese Sichtweise spreche die verfassungsrechtlich (Art. 2 Abs. 1 GG) verankerte Privatautonomie. Diesem Grundsatz folgend sollen die

⁹⁷ Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 Oktober 2019, S. 8.

⁹⁸ Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 Oktober 2019, S. 14 f.

Spindler/Schuster/Spindler/Dalby, *Recht d. elektron. Medien*, 4. Aufl. 2019, DS-GVO Art. 7 Rn. 12f; Ehmann/Selmayr/Heckmann/Paschke, *DS-GVO*, 2. Aufl., Art. 7 Rn. 96.

⁹⁹ Das Verhalten anderer Marktteilnehmer soll dem Verantwortlichen nicht zugerechnet werden, ferner sei eine echte „Gleichwertigkeit“ der verschiedenen Dienste nicht garantiert, s. EDPB (EDSA) Guidelines 5/2020, No. 38.

¹⁰⁰ Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 Oktober 2019, S. 9.

¹⁰¹ Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 Oktober 2019, S. 8.

¹⁰² Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 Oktober 2019, S. 9.

¹⁰³ Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 Oktober 2019, S. 9.

¹⁰⁴ Engeler, *ZD* 2018, 55, 57 f.

Parteien auch solche Pflichten vereinbaren können, zu deren Erfüllung die Verarbeitung von Daten notwendig ist.¹⁰⁵

Andere verweisen auf die nun in Art. 3 Abs. 1 S. 2 DI-RL expressis verbis genannte Möglichkeit, Verträge mit Daten als Zahlungsmittel zu schließen.¹⁰⁶ Eine solche „Zahlung mit Daten“ impliziere aber immer eine Einwilligung, die dann gegen das Kopplungsverbot verstoßen würde, da grade die Bereitstellung der Daten zur Bedingung für die Leistungserbringung gemacht würde.¹⁰⁷ Deshalb sollen nach dieser Auffassung solche Geschäftsmodelle durch Art. 6 Abs. 1 lit. b DS-GVO zu rechtfertigen sein, deren Wesen ein „Tausch Leistung gegen Daten“ ist.¹⁰⁸ Die Grenzen für die zulässigen Zwecke und Vereinbarungen wären demnach dann die des allgemeinen Vertragsrechts.

Hier kommt eine besondere Bedeutung der Abgrenzung zwischen Hauptleistungspflicht und Nebenabrede zu. Nur Nebenabreden unterliegen nach § 307 Abs. 3 BGB der Inhaltskontrolle des § 307 BGB.¹⁰⁹ Dafür kommt es darauf an, was die Parteien vereinbaren, insbesondere wie sich das Angebot des Verarbeiters für einen objektiven Empfänger darstellt: Handelt es sich um einen typischen „Leistung gegen Daten-Vertrag“ und wird dies auch transparent dargestellt, so wird die Bereitstellung der Daten regelmäßig eine Hauptleistungspflicht sein, die einer Inhaltskontrolle nach § 307 Abs. 3 BGB entzogen ist. Handelt es sich hingegen um einen klassischen Vertrag, z.B. Kauf von Waren gegen Entgelt, und versucht der Verkäufer durch Zusatz in seinen AGB eine Verarbeitung von Daten zu einem Zweck i. S. d. Art. 6 Abs. 1 lit. b DS-GVO zu erklären, kann dies der Inhaltskontrolle nach § 307 BGB unterliegen.¹¹⁰ Hier zeigt sich allerdings die Schwäche dieser Ansicht: Nach § 307 Abs. 2 Nr. 1 BGB sind solche Vereinbarungen unwirksam, die dem wesentlichen Grundgedanken gesetzlicher Regelungen widersprechen. Das wird in den meisten Fällen dazu führen, dass der zusätzlich vereinbarte Zweck, wenn er nicht zur Erfüllung einer im Vertrag vereinbarten Pflicht notwendig ist, wiederum nach § 307 BGB unwirksam ist.¹¹¹

Weiterhin könnten solche Zusatzvereinbarungen schon am Transparenzgebot scheitern oder als überraschende Klausel nach § 305c BGB unwirksam sein.¹¹²

Auch der EDSA erteilt dieser Ansicht eine eindeutige Absage: Nur solche Verarbeitungen seien von Art. 6 Abs. 1 b) DS-GVO gedeckt, die für die Erfüllung des konkreten Vertrags zwingend notwendig sind; der Verarbeitende muss also

¹⁰⁵ Engeler, ZD 2018, 55, 57 f.

¹⁰⁶ Zum Problem gegenüber der DS-GVO Bach, NJW 2019, 1705 (1706).

¹⁰⁷ So auch BeckOK Datenschutzrecht/Stemmer, 30. Ed. Stand 01.11.2019, Art.7 DS-GVO Rn. 41.1; zum Problem schon Dehmel/Hullen, ZD 2013, 147 (149 f).

¹⁰⁸ Dafür Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018 Art. 7 Rn. 51.

¹⁰⁹ MüKoBGB/Wurmnest, 8. Aufl. 2019, BGB § 307 Rn. 6 ff.

¹¹⁰ Wendehorst/Graf v. Westphalen, NJW 2016, 3745 (3748); Engeler, ZD 2018, 55 (57 f.); Simitis/Hornung/Spiecker gen. Döhmann/Klement, DS-GVO, 1. Aufl. 2019, Art. 6 Rn. 28; Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 37.

¹¹¹ Dazu Simitis/Hornung/Spiecker gen. Döhmann/Klement, DS-GVO, 1. Aufl. 2019, Art. 6 Rn. 27 ff; Hacker, ZfPW 2019, 148 (190 f).

¹¹² Simitis/Hornung/Spiecker gen. Döhmann/Klement, DS-GVO, 1. Aufl. 2019, Art. 6 Rn. 27; vgl. auch Härtig, CR 2016, 735 (740).

darlegen können, dass er den Vertragszweck ohne die Verarbeitung nicht erreichen kann.¹¹³ Dieser Zweck kann auch nicht künstlich durch Vertragsvereinbarung erweitert werden, etwa so, dass die Verwendung der Daten für personalisierte Werbung für die Erbringung seiner Leistung erforderlich ist.¹¹⁴ Als Beispiel für das Vorliegen einer echten Notwendigkeit lässt sich hingegen die Situation eines Online-Kaufs anführen: Um diesen erfolgreich abschließen zu können, ist die Mitteilung der Konto-/Kreditkartendetails für die Abwicklung der Zahlung unerlässlich.¹¹⁵ Der Vertragszweck Ware gegen Geld könnte also andernfalls nicht erreicht werden.

Dem EDSA ist letztlich zuzustimmen: Generell besteht die erhebliche Gefahr, die Vorgaben der DS-GVO durch eine weite Definition von Vertragszwecken zu verwässern und durch geschickte Vertragsgestaltung zu umgehen. Die oben geschilderte weite Auslegung des Art. 6 Abs. 1 lit. b DS-GVO ist daher abzulehnen.

Ferner konkretisiert ErwGr 43 DS-GVO die Freiwilligkeit dahin, dass diese zumindest unwahrscheinlich ist, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht und dieses Ungleichgewicht die Wahlfreiheit einschränkt. Ob die Einwilligung in diesem Fall tatsächlich freiwillig erfolgte, ist im Rahmen einer Einzelfallbetrachtung zu ermitteln.¹¹⁶ Eine solche liegt in jedem Fall bei der Anwendung von *vis absoluta* oder *vis compulsiva* zur Erlangung der Einwilligung vor.¹¹⁷ Ein klares Ungleichgewicht ist jedenfalls auch bei Subordinationsverhältnissen anzunehmen, etwa wenn eine Behörde handelt.¹¹⁸

Die Freiwilligkeit kann allerdings auch bei weniger intensiven Beeinträchtigungen ausgeschlossen sein. Ein gewisses Ungleichgewicht besteht so zum Beispiel zwar in der Regel auch zwischen einem Unternehmer und einem Verbraucher, da der Unternehmer im Regelfall über mehr Mittel und Gestaltungsspielraum verfügt. Dies allein wird aber nicht ausreichen, um einen freien Willen von Verbraucherinnen und Verbrauchern auszuschließen.¹¹⁹ Im Bereich der freien Wirtschaft können eine echte Monopolstellung¹²⁰ oder eine kartellähnliche Angebotslage¹²¹ die Freiwilligkeit in Frage stellen. Allerdings reicht hier das bloße Vorliegen eines Machtgefälles nicht aus; auch in Situationen einer strukturellen

¹¹³ Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 Oktober 2019, S. 9 Rn. 30.

¹¹⁴ Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 Oktober 2019, S. 10 Rn. 31.

¹¹⁵ für weitere Beispiele siehe Ehmann/Selmayr/Heckmann/Heberlein, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 13.

¹¹⁶ DSK Kurzpapier Nr. 20.

¹¹⁷ weiter geht Sydow, der die Legalisierungswirkung der Einwilligung gegenüber einer Behörde für generell ausgeschlossen hält, dies wäre aber eine Überdehnung des Wortlauts des ErwGr (43).

¹¹⁸ Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 7 Rn. 17; Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018 Art. 7 Rn. 42; Gierschmann ZD 2016, 51 (54); Paal/Pauly/Frenzel, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 19.

¹¹⁹ Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018 Art. 7 Rn. 44.

¹²⁰ Plath, BDSG/DS-GVO, 2. Aufl. 2016, Art. 7 Rn. 14; Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, Art. 7 Rn. 17; BeckOK Datenschutzrecht/Stemmer, DS-GVO, 30. Ed. 01.11.2019, Art. 7 Rn. 43; Krohm/Müller-Peltzer, ZD 2017, 551, (552, 554).

¹²¹ Ernst, ZD 2017, 110 (112); ähnlich Paal/Pauly/Frenzel, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 21 aE.

Machtasymmetrie führt dieser Umstand allein nicht zum generellen Ausschluss der Freiwilligkeit.¹²²

Vor dem Hintergrund des der Einwilligung immanenten Autonomieschutzes ist eine Freiwilligkeit auch in solchen Situationen zu bejahen, wenn der Betroffene effektiv die Möglichkeit hat, über das Ob und Wie der Datenverarbeitung zu bestimmen.¹²³ Insofern ist die Freiwilligkeit in keinem Lebensbereich generell zu verneinen. Daher kann sie anzunehmen sein, wenn ein Verantwortlicher z.B. eine marktbeherrschende Stellung aufgrund eines neuen, innovativen Geschäftsmodells hat.¹²⁴ Hier sollte die Freiwilligkeit nicht zu eng ausgelegt werden, um Anreize für Innovationen aufrecht zu erhalten. Einen weiteren wichtigen Abwägungsumstand bildet auch die Art der Leistung, so kann eine Zwangslage eher im Bereich der notwendigen Grundversorgung angenommen werden, als bei Anbietern von Luxusgütern. Diese Überlegung greift allerdings nicht, wenn das Datensubjekt einem gesetzlichen Kontrahierungszwang unterliegt, z.B. im Bereich der Pflichtversicherungen oder im Bereich der Energie- und Wasserversorgung, sodass die Pflicht zum Abschluss eines Vertrags die Freiwilligkeit entfallen lassen kann.¹²⁵

Es bedarf zusammenfassend also für die Frage der Freiwilligkeit einer Berücksichtigung aller Umstände im Einzelfall, insbesondere können hier auch der Umfang der Einwilligung und Verhandlungsmöglichkeiten eine Rolle spielen.¹²⁶ Eine Kopplung von Verarbeitung und angebotener Leistung kann hier ein starkes Indiz gegen eine Freiwilligkeit sein, bedingt diese jedoch nicht zwangsläufig. Es kommt vielmehr auch dabei auf die Transparenz und die entsprechende in Aussicht gestellte Gegenleistung an.

2.1.1.6. Jederzeitiger Widerruf

Spiegelbildlich zur Erteilung der Einwilligung berechtigt Art. 7 Abs. 3 DS-GVO die betroffene Person jederzeit, die Einwilligung ohne jegliche Begründung zu widerrufen. Der Widerruf der Einwilligung muss gem. Art. 7 Abs. 3 S. 4 DS-GVO „so einfach wie die Erteilung sein“, dies bezieht sich auf den Widerrufsakt selbst, ebenso wie auf die Auffindbarkeit und Verständlichkeit der Widerrufsbelehrung.¹²⁷ Ferner darf der Widerruf nach zutreffender Ansicht des EDSA nicht an zusätzliche Gebühren oder mit einer Absenkung des Leistungsniveaus verknüpft sein.¹²⁸ Dies bedeutet allerdings nicht, dass damit schuldrechtliche bzw. vertragsrechtliche Verpflichtungen des Diensteanbieters weiter bestehen bleiben; sind die Daten nicht (!) erforderlich für die Durchführung eines Vertrags (liegt also keine Rechtfertigung nach Art. 6 Abs. 1 b DS-GVO vor) und werden zusätzliche Dienste mit Daten „bezahlt“, wie es Art. 3 Abs. 1 S. 2 DI-RL vorsieht, kann

¹²² Sydow/Ingold, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 28.

¹²³ Vgl. Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018 Art. 7 Rn. 44.

¹²⁴ S. Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 22f; Paal/Pauly/Frenzel, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 18.

¹²⁵ Simitis/Hornung/Spiecker gen. Döhmann/Klement, DS-GVO, 1. Aufl. 2019, Art. 7 Rn. 62.

¹²⁶ Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 42 ff;

¹²⁷ Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 91 f.; Simitis/Hornung/Spiecker gen. Döhmann/Klement, DS-GVO, 1. Aufl. 2019, Art. 7 Rn. 85 ff.; Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, Art. 7 Rn. 11.

¹²⁸ EDPB (EDSA) Guidelines 5/2020, No. 114; Schantz/Wolff/Wolff, DatenschutzR, 1. Aufl. 2017, Rn. 532.

der Widerruf zur Einstellung der Dienste führen.¹²⁹ Deshalb wird teilweise vertreten, dass das Widerrufsrecht in solchen Fällen nach Treu und Glauben ausgeschlossen sein soll, in denen sonst sofort wieder auf Grund vertraglicher Verpflichtungen eine Einwilligung zu erteilen wäre (*dolo agit*-Einrede).¹³⁰ Entsprechend des Wortlauts der DS-GVO und der grundsätzlichen Unabdingbarkeit dieser Vorschriften¹³¹ ist der Widerruf der Einwilligung in der Regel gleichzeitig als Kündigung des verknüpften Dienstes zu verstehen.¹³² Damit wird dem Umstand Rechnung getragen, dass im Falle einer Zahlung mit Daten und einer Inanspruchnahme von Diensten regelmäßig keine Rückabwicklung möglich ist, was auch explizit in der DI-RL zum Ausdruck kommt.¹³³ Dass vom Betroffenen keinerlei Unannehmlichkeiten bzw. geringfügige negative Folgen hinzunehmen sind, wie der Wegfall einer Kostensubventionierung, ist jedenfalls abzulehnen,¹³⁴ auch deshalb, damit nicht bei Annahme eines „weichen“ Kopplungsverbotes über den Weg des Widerrufs schlussendlich doch ein Hindernis für solche Geschäftsmodelle bestünde.

Da wie bereits beschrieben die Erteilung einer differenzierten Einwilligung (s. oben 2.1.1.3) nach der DS-GVO erforderlich ist, ist dem Betroffenen gleichsam die Möglichkeit eines differenzierten Widerrufs einzuräumen.¹³⁵

Obwohl die DS-GVO dies nicht explizit vorschreibt, plädiert der EDSA mit guten Gründen dafür, dass der Widerruf mit den gleichen Mitteln bewerkstelligt werden können muss, wie die Erteilung der Einwilligung, z.B. mittels derselben Schnittstelle oder über dieselbe Funktion des Nutzerkontos, da den Betroffenen andernfalls eine unangemessene Anstrengung aufgelastet würde.¹³⁶ Wurde zur Einwilligungserteilung eine „Tick-Box“ genutzt, sollte demnach auch das Setzen eines Häkchens ausreichen, um die Einwilligung zurückzuziehen. Insbesondere sollten Verantwortliche darauf achten, dass eine elektronisch erteilte Einwilligung, stets auch elektronisch widerrufen werden kann – und Betroffene nicht auf den analogen Postweg verwiesen werden.¹³⁷

Der Widerruf der Einwilligung hat *ex-nunc*-Wirkung.¹³⁸ Die Rechtmäßigkeit der Verarbeitung bereits vor dem Widerruf erhobener personenbezogener Daten

¹²⁹ Metzger, AcP 216 (2016), 818 (834): für mögliche schuldrechtliche Lösungswege Sattler, JZ 2017, 1036 (1040 f.)

¹³⁰ Simitis/Hornung/Spiecker gen. Döhmman/Klement, DS-GVO, 1. Aufl. 2019, Art. 7 Rn. 92; Gola/Schulz DS-GVO, 2. Aufl. 2018, Art. 7 Rn 57; Spindler, DB 2016, 937 (940);

¹³¹ Gola/Schulz DS-GVO, 2. Aufl. 2018, Art. 7 Rn 5; zum Schadensersatz Taeger/Gabel/Moos/Schefzig, DS-GVO, 3. Aufl. 2019, Art. 82 Rn 53.

¹³² Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 7 Rn. 13.

¹³³ Art. 16 DI-RL; ErwGr 69 DI-RL; dazu Spindler/Sein, MMR 2019, 488 (491).

¹³⁴ Ebenso Gola/Schulz DS-GVO, 2. Aufl. 2018, Art. 7 Rn 55.

¹³⁵ Ebenso Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 35; Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 91.

¹³⁶ EDPB (EDSA) Guidelines 5/2020, No. 114; Gola/Schulz DS-GVO, 2. Aufl. 2018, Art. 7 Rn 56; Ehmann/Selmayr/Heckmann/Paschke, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 91.

¹³⁷ Gleiches gilt für mündl. Einwilligungen, diese müssen auch mündlich widerrufen werden können; die Pflicht zu Benennung einer Vorgangsnummer stellt ebenfalls eine übergebührende Belastung dar, s. Paal/Pauly/Frenzel, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 16-17 m.w.N.

¹³⁸ Simitis/Hornung/Spiecker gen. Döhmman/Klement, DS-GVO, 1. Aufl. 2019, Art. 7 Rn. 90; Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 7 Rn. 11; Veil NJW 2018, 3337 (3341).

bleibt mithin vom Widerruf unberührt.¹³⁹ Trotz Widerrufs darf die Einwilligung insbesondere zu Beweis Zwecken gespeichert werden.¹⁴⁰

2.1.1.7. Besondere Einwilligungen: Minderjährige

Für Minderjährige bzw. Kinder sieht die DS-GVO in Art. 8 besondere Voraussetzungen vor, die zusätzlich zu den allgemeinen Bedingungen einer Einwilligung vorliegen müssen.¹⁴¹ Unter der Grenze von 16 Jahren müssen die Eltern bzw. Erziehungsberechtigten in die Datenverarbeitung einwilligen oder der Einwilligung des Kindes zustimmen, wobei für die Mitgliedstaaten nach Art. 9 Abs. 1 Abs. 2 DS-GVO die Möglichkeit besteht, ein niedrigeres Alter festzulegen. Deutschland hat hiervon bislang keinen Gebrauch gemacht (§ 51 BDSG). Die absolute Mindestgrenze von 13 Jahren darf allerdings nicht unterschritten werden.

Der Anwendungsbereich des Art. 8 DS-GVO erstreckt sich auf Dienste der Informationsgesellschaft¹⁴², die sich direkt und gezielt an Kinder richten, wobei etwa die kindgerechte Illustration, Bebilderung, Sprache und der Inhalt zur Abgrenzung dienen.¹⁴³ Soweit sich der Dienst sowohl an volljährige Personen als auch an Kinder richtet („Dual-use“), oder keine eindeutige Zielgruppe erkennen lässt (z.B. soziale Netzwerke), sollte von einem Angebot, das (auch) an Kinder gerichtet ist, ausgegangen werden.¹⁴⁴

Die Zustimmung der Eltern in die Einwilligung des Minderjährigen könnte abermals per Double-Opt-in erfolgen, indem sie dem Verantwortlichen gesondert (via SMS, E-Mail o. a.) die getätigte Einwilligung bestätigen.¹⁴⁵

Der EDSA verlangt in diesem Zusammenhang von den Verantwortlichen, „angemessene Anstrengungen“ bzw. Kontrollen zu unternehmen, um die Altersangabe der betroffenen Person zu überprüfen.¹⁴⁶ Gleiches gilt für die Erteilung der Einwilligung durch einen Träger der elterlichen Verantwortung; auch hier soll sich der Verantwortliche vergewissern, ob „die Person, die diese Einwilligung erteilt, tatsächlich Träger der elterlichen Verantwortung ist.“¹⁴⁷ Bei geringen Risiken hält der EDSA es aber für ausreichend, dass eine Altersangabe oder das Ausfüllen eines Formulars gefordert wird,¹⁴⁸ hinsichtlich der elterlichen Einwilligung eine Bestätigung per E-Mail.¹⁴⁹

¹³⁹ Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 36; Sydow/Ingold, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 48, Schantz/Wolff//Wolff, DatenschutzR, 1. Aufl. 2017, Rn. 531.

¹⁴⁰ LG Hamburg, Urt. v. 20.12.2008 – 312 O 362/08.

¹⁴¹ Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 8 Rn. 3; Simitis/Hornung/Spiecker gen. Döhmner/Klement, DS-GVO, 1. Aufl. 2019, Art. 7 Rn. 10; Joachim ZD 2017, 414.

¹⁴² Im Sinne der Richtlinie 2015/1535 gem. Art. 4 Abs. 25 DS-GVO.

¹⁴³ Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 8 Rn. 15.

¹⁴⁴ EDPB (EDSA) Guidelines 5/2020, No. 130; Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 8 Rn. 6 f.

¹⁴⁵ Ebenso Möhrke-Sobolewski/Klas K&R 2016, 373 (377); Buchner/Kühling DuD 2017, 544 (547); f. einen Überblick über weitere Zustimmungsmethoden, s. Rauda, MMR 2017, 15 (18f.); Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 8 Rn. 10.

¹⁴⁶ EDPB (EDSA) Guidelines 5/2020, No. 132 f.

¹⁴⁷ EDPB (EDSA) Guidelines 5/2020, No. 134.

¹⁴⁸ EDPB (EDSA) Guidelines 5/2020, No. 135.

¹⁴⁹ EDPB (EDSA) Guidelines 5/2020, No. 137

2.1.1.8. Dauer der Einwilligung

Die DS-GVO enthält keine zeitliche Beschränkung der Einwilligung, solange sich die Zwecke der Datenverarbeitung nicht ändern; bei einer Zweckänderung ist selbstverständlich eine neue Einwilligung erforderlich.¹⁵⁰

Insbesondere gelten nach ErwGr 171 S. 3 auch vor Inkrafttreten der DS-GVO erteilte Einwilligungen weiter, sodass diese nicht erneuert werden müssen.¹⁵¹

Der EDSA spricht sich jedoch dafür aus, dass es einer „bewährten Praxis“ entspreche, dass die Einwilligung in bestimmten Zeitabschnitten erneuert würde – auch wenn sich der Zweck nicht geändert habe.¹⁵² Gleichzeitig darf diese routinemäßige Einwilligungsaktualisierung die obengenannte Einwilligungsmüdigkeit keinesfalls zusätzlich verstärken.

2.1.1.9. Neue Einwilligungsmechanismen

Dass die Digitalisierung aller Lebensbereiche und der damit verbundene Zuwachs einwilligungsbedürftiger Datenverarbeitungen eine zeitgemäße Einwilligungseinholung erfordert, hat den EDSA veranlasst, zu Fragen des Einwilligungsmanagements im Hinblick auf digitale Dienstleistungen näher Stellung zu nehmen¹⁵³ – was für die Praxis der Aufsichtsbehörden naturgemäß von eminenter Bedeutung ist. Entsprechend den Anforderungen werden später die konkreten Einwilligungsmanagementsysteme in der Praxis nochmals gesondert rechtlich bewertet; die nachfolgenden Ausführungen dienen einer zunächst abstrakten Näherung.

2.1.1.9.1. Anforderungen an Einwilligungsmanagement

Der EDSA stellt klar, dass es den Verantwortlichen unbenommen ist, neue Einwilligungsmechanismen zu entwickeln, solange sie die Vorgaben der DS-GVO beachten.¹⁵⁴ Diese Klarstellung spiegelt die explizite Technologieneutralität der DS-GVO wider.¹⁵⁵ Insbesondere die zunehmende Verbreitung sensor-gesteuerter IT, wie berührungsempfindliche Bildschirme oder kameraunterstützte Geräte, bietet Potenzial für neue und effiziente Formen der Einwilligungserteilung, denn auch eine physische Handlung kann als eindeutige bestätigende Handlung angesehen werden, die mit der DS-GVO konform ist.¹⁵⁶ Diesbezüglich nennt der EDSA eine nicht abschließende Liste von Beispielen zulässiger Einwilligungsgesten, wie das Wischen über den Bildschirm, das Drehen eines Smartphones o.ä. sofern der Betroffene im Voraus angemessen über die Bedeutung seiner Handlung informiert wurde.¹⁵⁷

¹⁵⁰ Information Commissioner`s Office, „Consent“, vers. 1.0.57, S. 29, 32 f.

¹⁵¹ Anders wohl aber OLG Frankfurt/M, Urt. v. 27.6.2019 – 6 U 6/19, ZD 2019, 507 Rn. 10 mit abl. Anm. Eckardt et al.

¹⁵² EDPB (EDSA) Guidelines 5/2020, No. 111

¹⁵³ EDPB (EDSA) Guidelines 5/2020, No. 87 ff-.

¹⁵⁴ EDPB (EDSA) Guidelines 5/2020, No. 83..

¹⁵⁵ S. ErwGr 15 DS-GVO, weiterf. zur technologieneutralen Ausrichtung der DS-GVO, s. Spindler/Schuster/Spindler/Dalby, Recht d. elektron. Medien, 4. Aufl. 2019, DS-GVO Art. 2 Rn. 3.

¹⁵⁶ EDPB (EDSA) Guidelines 5/2020, No. 83.

¹⁵⁷ EDPB (EDSA) Guidelines 5/2020, No. 85 f-.

In jedem Fall muss der Einwilligungshandlung ein unzweifelhafter Erklärungswert (und -bewusstsein) beigemessen werden können,¹⁵⁸ weshalb es aus Betroffenen­sicht einer unzweideutigen und unmissverständlichen Ausgestaltung bedarf:

„Controllers should design consent mechanisms in ways that are clear to data subjects. Controllers must avoid ambiguity and must ensure that the action by which consent is given can be distinguished from other actions. Therefore, merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation.“¹⁵⁹

Daher erfüllt das bloße Scrollen über eine Website als allzu gewöhnliche Nutzungshandlung nicht die Voraussetzungen einer unmissverständlichen Handlung.¹⁶⁰ Folgt man der Ansicht der Aufsichtsbehörden, kann mithin auch die Fortsetzung eines Telefonats nach vorheriger Information über die Anfertigung eines Mitschnitts nicht als eindeutig bestätigende Handlung ausreichen.¹⁶¹

2.1.1.9.2. Problem: Gewöhnungseffekte

Die Erbringung digitaler Dienstleistungen setzt häufig die Verarbeitung personenbezogener Daten voraus, sei es, weil sich die Dienstleistung selbst auf die Verarbeitung von Nutzerdaten erstreckt (so z.B. beim Tracking von Fitness-Daten),¹⁶² weil der Dienstanbieter seine Leistungserbringung mit Gewinnerzielungsabsicht an die Gestattung der wirtschaftlichen Verwertung der Betroffenen­daten knüpft (so etwa beim Web-Tracking zu Zwecken des personalisierten Online-Marketings),¹⁶³ oder sei es eine Kombination aus beidem (z.B. bei der Nutzung sozialer Netzwerke).¹⁶⁴

Nutzerinnen und Nutzer digitaler Inhalte sehen sich daher täglich und wiederkehrend zahlreichen Einwilligungsaufforderungen ausgesetzt:¹⁶⁵

„This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.“¹⁶⁶

Es besteht daher berechtigterweise die große Sorge, dass Nutzerinnen und Nutzer aufgrund der schieren Flut an Einwilligungersuchen eine Einwilligungsroutine ausbilden und die bereitgestellten Informationen nicht länger zur Kenntnis

¹⁵⁸ Zum Erklärungsbewusstsein, s. Kühling/Buchner/Buchner/Kühling, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 56.

¹⁵⁹ EDPB (EDSA) Guidelines 5/2020, No. 84.

¹⁶⁰ EDPB (EDSA) Guidelines 5/2020, No. 86; Ehmann/Selmayr/Klabunde, DS-GVO, 2. Aufl., Art. 4 Rn. 53.

¹⁶¹ Dem ist zuzustimmen, da es ein Leichtes ist den Betroffenen telefonisch zu einem Tastendruck oder einer bestätigenden Aussage aufzufordern und hierdurch das Risiko einer überhörten Belehrung zu minimieren; a.A. Krohm ZD 2016, 368 (372).

¹⁶² Kühling/Buchner/Weichert, DS-GVO, 2. Aufl. 2018, Art. 9 Rn. 34 ff.; weiterf. zum Datenschutz in der Gesundheitsbranche, Werry/Knoblich MPR 2017, 1; Weichert MedR 2019, 622.

¹⁶³ Schirnbacher ITRB 2016, 274 (277 ff.); Golland MMR 2018, 130 (133).

¹⁶⁴ So bereits Erd NVwZ 2011, 19.

¹⁶⁵ So auch ErwGr 22 S. 2 e-Privacy-VO-E.

¹⁶⁶ EDPB (EDSA) Guidelines 5/2020, No. 87.

nehmen. Aufgrund dessen, dass sich aus Sicht des EDSA Einwilligungsaufforderungen in der Regel auf Verarbeitungen erstrecken, die andernfalls rechtswidrig sind, nimmt der EDSA die Verantwortlichen in die Pflicht: „The GDPR places upon controllers the obligation to develop ways to tackle this issue“.¹⁶⁷

Generell ist der Bewertung des EDSA zuzustimmen, dass die gesteigerte Menge an Einwilligungsersuchen den beabsichtigten Warneffekt schmälert, doch sind auch jene Stimmen nachvollziehbar, die eine übergebührlige Bevormundung der Betroffenen mit dem Verweis darauf ablehnen, dass sich die Betroffenen durch vorschnelles „Weiterklicken“ eigenverantwortlich der eigenen Informiertheit beraubten, es also letztlich immer noch um eine privatautonome Handlung geht.¹⁶⁸

Zudem kann eine Pflicht zur Vermeidung von zahlreichen Einwilligungen dem Wortlaut der DS-GVO nicht entnommen werden. Art. 7 enthält dazu keinerlei Aussagen, es besteht lediglich die Pflicht zur verständlichen und leicht zugänglichen Form. Es scheint überdies nicht interessengerecht, denjenigen, die gesetzlich verpflichtet sind, Einwilligungen einzuholen, die Korrektur der negativen Folgen aufzuerlegen, wenn eine Einwilligung eingeholt wird.

Ein Ansatz, um mögliche Einwilligungsroutrinen zu vermeiden, bestünde in der personalisierten, „granularen“ Einwilligungsaufforderung, die den persönlichen Besonderheiten des Betroffenen Rechnung trägt und im positiven Sinne „Nudging“ betreibt,¹⁶⁹ um eintretender Routine entgegenzuwirken – was hier nicht in extenso vertieft werden kann, jedoch im Abschnitt 2.1.2 zur verhaltenswissenschaftlichen Perspektive diskutiert wird. Denkbar wäre dies u.a. durch die Nutzung sich abwechselnder Gesten (Wischen, Winken, Muster-Zeichnen, Anklicken, etc.) zur Einwilligungserteilung. Allerdings setzt eine granuläre, personalisierte Einwilligungsmanagement seinerseits oft voraus, dass bereits entsprechende Profile über den Betroffenen vorliegen – was dann wiederum datenschutzrechtlichen Bedenken unterliegt.

Eine andere Lösung dieses Problems könnte darin bestehen, dort anzusetzen, wo Einwilligungen erfragt werden, obwohl diese für eine rechtmäßige Verarbeitung gar nicht erforderlich sind. Das betrifft die Fälle, in denen ein Verarbeiter „lieber auf Nummer sicher“ geht und eine Einwilligung einholt¹⁷⁰, obwohl eine Verarbeitung z.B. zur Erfüllung des Vertrags notwendig ist und deshalb schon eine Berechtigung nach Art. 6 Abs. 1 lit. b besteht.¹⁷¹ Dadurch, dass nach (allerdings strittiger) Auffassung des EDSA dem Verarbeitenden im Nachhinein die Möglichkeit verwehrt wird, sich alternativ auf den einschlägigen Zulässigkeitstatbestand zu berufen und so ein Widerruf der Einwilligung des Betroffenen dazu

¹⁶⁷ EDPB (EDSA) Guidelines 5/2020, No. 96.

¹⁶⁸ S. z.B. *Körber* NZKart 2016, 348 (350)

¹⁶⁹ Dazu umfassend *Herfurth/Benner-Tischler*, ZD-Aktuell 2017, 05901; zum Datenschutz-Nudging im Arbeitsverhältnis *Schomberg/Barev/Janson/Hupfeld*, DuD 2019, 774.

¹⁷⁰ Ausf. dazu <https://www.datenschutzbeauftragter-info.de/die-verschlimmbesserung-der-einwilligung-nach-dsgvo/> (abgerufen am: 13.12.2019).

¹⁷¹ *Stolz*, in: *Vertragsformulare Premium Teil 13 IT- und Datenschutzrecht*, Stand 01.11.2019, 13.8.2.2 Rn. 2; die hessische Datenschutzbehörde schlägt in ihrem FAQ zur DS-GVO sogar vor bei Unsicherheit eine Einwilligung vorsorglich einzuholen, um die Folgen von potentiellen Datenschutzverstößen zu vermeiden <https://datenschutz.hessen.de/infothek/h%C3%A4ufig-gestellte-fragen-hgf> (abgerufen am: 13.12.2019).

führt, dass keine Verarbeitung mehr möglich ist,¹⁷² wird letztlich der Verarbeiter dazu angehalten, Einwilligungen zu reduzieren.

2.1.1.9.3. Zentralisierte Erteilungs- und Widerrufsmöglichkeiten (PIMS)

Ein grundsätzlich anderer Ansatz könnte darin bestehen, den Betroffenen zentralisiertere Informations- und Einwilligungstools (sog. Personal Information Management Systems (PIMS)) zur Verfügung zu stellen, die es ihnen besonders benutzerfreundlich erlauben, Einwilligungen zu verwalten.¹⁷³

Tools zur zentralisierten Einwilligungsverwaltung müssten zwar nicht - könnten jedoch - in eine bestehende Software (wie einen Browser) eingebettet werden. Eigenständige Software-Lösungen wären nur praktikabel, soweit die einwilligungsbedürftigen Dienste eine Schnittstelle zu dem genutzten Verwaltungssystem besäßen, um das Vorliegen einer sachgleichen Einwilligung feststellen zu können, bzw. eine Neuerteilung zu initiieren.

Genau wie für die Individual-Einwilligung müsste jedwedes zentralisierte Einwilligungsmanagementsystem die zuvor genannten Wirksamkeitsvoraussetzungen der Einwilligung (Form, Fallbezogenheit, Informiertheit, Freiwilligkeit etc.) erfüllen und einen eindeutig-bestätigenden Erteilungsmechanismus aufweisen. Insbesondere an die Granularität wären diesbezüglich hohe Anforderungen zu stellen, damit konkrete („fallbezogene“) Verarbeitungen transparent voneinander differenziert werden können, ohne zu einer Unübersichtlichkeit zu führen.¹⁷⁴

Zum einen könnte der Betroffene bei der erstmaligen Datenverarbeitung eine Einwilligung erteilen, die dann (ebenfalls mit seinem Einverständnis) im Browser oder einem anderen hierfür vorgesehenen Programm hinterlegt wird. Für sachgleiche Verarbeitungen (mit denselben Zwecken und Mitteln durch denselben Verantwortlichen) könnte sodann die abgespeicherte Einwilligung fruchtbar gemacht werden. Ein Verstoß gegen die auf einen konkreten Zweck bezogene Einwilligung wäre damit nicht verbunden, wenn der Zweck und die Verarbeitung identisch mit der ersten Verarbeitung sind.

Zum anderen könnte eine verarbeitungsbezogene Informiertheit des Betroffenen auch dadurch gewährleistet werden, dass der Betroffene ohne konkreten Verarbeitungsanlass (also ohne Bezug zu einer unmittelbar bevorstehenden Verarbeitung seiner Daten durch einen bekannten Verantwortlichen) detailliert beschriebene Einwilligungen in zukünftige Verarbeitungsszenarien erteilt. So wäre es denkbar, dass der Betroffene festlegt, dass er in die Speicherung seiner

¹⁷² EDPB (EDSA) Guidelines 5/2020, No. 121 ff.; für eine solche „Sperrung“ auch *Kühling/Buchner/Buchner/Kühling*, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 18, die ein solches Gebaren als unzulässiges widersprüchliches Verhalten kategorisieren.

¹⁷³ Für einen ausführlichen Überblick über technische Konzepte, s. *Riechert*, in der Studie zum Datenschutz durch PIMS von 2016 „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“ des Stiftung Datenschutz, Stellungnahme B Anhang 1 S. 5, abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_rechtliche_Stellungnahme_ePrivacy_Richtlinie_final_01.pdf, zuletzt abgerufen am 18.11.2019.

¹⁷⁴ ebenso *Riechert*, in der Studie zum Datenschutz durch PIMS von 2016 „Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen“ des Stiftung Datenschutz, Stellungnahme B Anhang 1 S. 46 f., abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_rechtliche_Stellungnahme_e-Privacy_Richtlinie_final_01.pdf, zuletzt abgerufen am 18.11.2019.

Browserdaten durch Tracking-Cookies und die Verwendung seiner E-Mail-Adresse zum Zwecke der werblichen Ansprache durch die Betreiber eines besuchten Webshops zustimmt. In einem weiteren Schritt wäre es erforderlich, dass der Betroffene aus einem Katalog bekannter Webshop-Betreiber potenzielle Verantwortliche (im Sinne einer „Whitelist“) auswählt, für deren Seiten die Einwilligung gelten solle. Weniger bekannte Anbieter müssten hingegen auf den erstgenannten Mechanismus zurückgreifen.

Diese neuen, zentralisierteren Formen der Einwilligungserteilung könnten dazu dienen „Abnutzungserscheinungen“ durch widerkehrende Einwilligungshandlungen und -aufforderungen entgegenzuwirken und gerade aufgrund der reduzierten Mitwirkungsbedürftigkeit des Betroffenen dessen Recht auf informationelle Selbstbestimmung zu stärken.

Obwohl auch hier die Gefahr von Gewöhnungseffekten besteht, sieht der EDSA in Browsereinstellungen einen ggf. zulässigen Einwilligungsmechanismus:¹⁷⁵

„An often-mentioned example to do this in the online context is to obtain consent of Internet users via their browser settings. Such settings should be developed in line with the conditions for valid consent in the GDPR, as for instance that the consent shall be granular for each of the envisaged purposes and that the information to be provided, should name the controllers“

Allerdings setzt dies die vorherige Kenntnis des Betroffenen von den Datenverarbeitungsvorgängen voraus. Inwiefern dies tatsächlich mit solchen ex-ante Einwilligungen in Browser erfolgen kann, erscheint jedoch zweifelhaft: Schon wenn mehrere Nutzerinnen und Nutzer ein Endgerät gemeinschaftlich nutzen (was für den Verantwortlichen nicht erkennbar sein muss), ist für den Verantwortlichen nicht nachvollziehbar, welche Nutzerin bzw. welcher Nutzer die Voreinstellung getätigt hat.¹⁷⁶ Zudem müsste der Dienst stets einen alternativen Einwilligungsmechanismus für Betroffene bereithalten, die keine derartigen Voreinstellungen vorgenommen haben.¹⁷⁷ Auch ist fraglich, ob die ex-ante zu treffenden Einwilligungen tatsächlich dem Erfordernis des auf die konkrete Datenverarbeitung bezogenen Zwecks sowie des Verantwortlichen entsprechen können; abstrakte bzw. generische Einwilligungen sieht die DS-GVO gerade nicht vor.

Etwas anderes könnte sich de lege ferenda nach Art. 8 Abs. 1 lit. b e-Privacy-VO-E in Verbindung mit ErwGr 22 S. 5 e-Privacy-VO-E ergeben, der den Einsatz von Cookies etc. explizit erlaubt, sofern Nutzerinnen und Nutzer dies - ggf. durch eine zentralisierte Einwilligung in den Einstellungen des Endgerätes (z.B. des Browsers) – gestatten.¹⁷⁸

2.1.1.10. Zusammenfassung

In einer vergrößernden Sicht lassen sich die rechtlichen Anforderungen in der Weise zusammenfassen, dass gerade bei online-Diensten eine auf den konkreten Datenverarbeitungsvorgang bezogene Information erforderlich ist, diese unmissverständlich und klar zu erteilen ist, der Betroffene die freie Wahl haben

¹⁷⁵ EDPB (EDSA) Guidelines 5/2020, No. 89.

¹⁷⁶ Forgó/Helfrich/Schneider/Arning/Born, Betrieblicher Datenschutz, 3. Aufl. 2019, Kapitel 2 Rn. 81.

¹⁷⁷ Forgó/Helfrich/Schneider/Arning/Born, Betrieblicher Datenschutz, 3. Aufl. 2019, Kapitel 2 Rn. 81.

¹⁷⁸ Forgó/Helfrich/Schneider/Arning/Born, Betrieblicher Datenschutz, 3. Aufl. 2019, Kapitel 2 Rn. 81.

muss, ob er einwilligt oder nicht, ohne Nachteile (insbesondere der Koppelung mit einer vertraglichen Leistung, ohne dass die Daten erforderlich sind) befürchten zu müssen und schließlich jederzeit widerrufen kann. Besondere Probleme, die nur im Einzelfall gelöst werden können, weist damit das angesprochene Koppelungsverbot des über die reine Vertragserfüllung hinausgehenden Angebots von Leistungen im Austausch gegen die Einwilligung zur Preisgabe von personenbezogenen Daten auf. Einwilligungsmanagementsysteme müssen insbesondere die vor der Datenverarbeitung zu erteilende Information des Einwilligenden berücksichtigen; ex-post Änderungen oder Modifizierungen genügen nicht.

2.1.2. Verhaltenswissenschaftliche Perspektive

Da das zu entwickelnde Einwilligungsmanagementsystem nicht nur rechtskonform, sondern auch nutzerfreundlich sein soll, werden im folgenden Abschnitt die verhaltenswissenschaftlichen Aspekte vorgestellt, die für die Bewertung von Einwilligungsmodellen relevant sind. Zum einen werden Aspekte des Human Centered Design (HCD) diskutiert, die bei der Entwicklung von Softwarelösungen im Allgemeinen berücksichtigt werden sollten. Zum anderen werden einwilligungsrelevante Aspekte beschrieben, die sich auf konkrete Einwilligungssituationen beziehen.

2.1.2.1. Human Centered Design

Nach Maguire (2001) ist HCD das Einbeziehen der Nutzerperspektive in die Entwicklung von Softwarelösungen, um ein nutzerbasiertes System zu erhalten. Übergeordnet sind dabei die Aspekte der **einfachen Erlernbarkeit und Nutzung** relevant, so dass Nutzerinnen und Nutzer ein System zur Verfügung gestellt wird, das sich an ihre bevorzugte Nutzung anpasst.

Darüber hinaus gibt es eine Reihe weiterer HCD-Aspekte, die für das Nutzungserlebnis eine Rolle spielen. Zu ihnen zählen

- Anpassbarkeit / Einstellungsmöglichkeiten
- Vertrauenswürdigkeit
- Informiertheit
- Komplexität
- Übersichtlichkeit¹⁷⁹

Nach Maguire (2001) ist die Optimierung des HCD aus mehreren Gründen von Vorteil für die Entwicklung von Softwarelösungen:

1. Ein optimales HCD sorgt dafür, dass Nutzerinnen und Nutzer weniger Training und Support bei der Nutzung benötigen,
2. sie sich auf die Aufgabe konzentrieren können und nicht auf das System an sich, was die Produktivität erhöht und

¹⁷⁹ Die Faktoren leiten sich dabei aus der HCD- und Usability-Literatur ab und werden ausführlich in Winter et al. (2015), Laugwitz et al. (2009) und Figl (2010) abgeleitet und beschrieben. Die behandelten, einwilligungsrelevanten Aspekte sind dabei lediglich eine Teilmenge aller für die Nutzererfahrung relevanten Aspekte.

3. Inkonsistenzen bzw. Fehler bei der Nutzung reduziert werden.

Des Weiteren wirkt sich HCD auch auf die Wahrnehmung der Anwendung bzw. des Anbieters aus:

4. Ein einfacher Zugang zur Anwendung selbst steigert so die Akzeptanz der Anwendung und
5. positives Feedback durch die Nutzerinnen und Nutzer verbessert die allgemeine Reputation.

2.1.2.2. *Einwilligungsrelevante Aspekte*

Neben übergeordneten Parametern, die sich aus der Optimierung des HCD für Software-Lösungen ableiten, sind weitere Faktoren relevant, die für die Einwilligungssituation spezifisch sind. Diese werden im folgenden Abschnitt vorgestellt und genauer erläutert.

2.1.2.2.1. *Aufbereitung der Informationen und Texte*

Nach Friedman et al. (2005) müssen für das Modell der informierten Einwilligung aus verhaltenswissenschaftlicher Perspektive mehrere Anforderungen erfüllt sein. Hierzu zählen akkurate und explizite Informationen, die den (kognitiven) Fähigkeiten der Nutzerinnen und Nutzer entsprechen und korrekt genutzt werden können. Kettner et al. (2018) definieren deshalb sog. DSE-inhärente¹⁸⁰ Faktoren, die auf die Informiertheit wirken und gestalterisch beeinflusst werden können:

Zum einen ist bei Datenschutzinformationen im Allgemeinen die *Textlänge*, d.h. die Wortanzahl, Zeichenanzahl und der Seitenumfang relevant. Je länger Datenschutztexte, desto geringer die Wahrscheinlichkeit, dass Verbraucherinnen und Verbraucher die Texte tatsächlich (vollständig) lesen und somit verarbeiten.¹⁸¹ Jedoch steht dieses Ergebnis der gesteigerten Lesewahrscheinlichkeit in einem Spannungsverhältnis mit der Anforderung, einen akkuraten und somit vollständigen Text zur Verfügung zu stellen. Bei einer großen Anzahl v.a. technischer Verarbeitungsprozesse ist es teilweise notwendig, ausführliche Erklärungen bereitzustellen, damit keine relevanten Informationen verlorengehen.

Neben dem Umfang der Texte spielt laut Kettner et al. (2018) auch der *Schwierigkeitsgrad der verwendeten Sprache* eine Rolle. Dieser definiert sich als die durchschnittliche Satz- und Wortlänge sowie über die Verwendungshäufigkeit von technischen und juristischen Fachbegriffen und einer leichten versus komplexen Sprache.¹⁸² Je höher der Schwierigkeitsgrad der Texte an sich, desto geringer ist die Wahrscheinlichkeit, dass Verbraucherinnen und Verbraucher durch die Texte tatsächlich informiert sind.

¹⁸⁰ DSE Abkürzung für Datenschutzerklärung

¹⁸¹ Dies konnte in einem verhaltenswissenschaftlichen Experiment von Kettner et al. (2018) bestätigt werden. So wurde die Lesewahrscheinlichkeit der Experimentalteilnehmerinnen und -teilnehmer für unterschiedlich lange Versionen einer Datenschutzerklärung getestet. Die Langversion schnitt bei der Lesewahrscheinlichkeit signifikant schlechter ab als die Kurzversion der Datenschutzerklärung.

¹⁸² Leichte Sprache verwendet bspw. aktive und indikative Sätze und vermeidet doppelte Verneinungen.

2.1.2.2.2. Framing

Ein weiterer Aspekt, der in Friedmans Modell der informierten Einwilligung berücksichtigt wird, ist *Comprehension* (dt. Verständnis und Auffassungsvermögen). Dieser Aspekt beschreibt bzw. definiert, ob Nutzerinnen und Nutzer die bereitgestellte Information tatsächlich akkurat interpretieren. Neben der oben genannten Vollständigkeit und Korrektheit der Information ist dieser Aspekt eng mit dem sogenannten *Framing* (dt. Rahmung) verknüpft und kann das Entscheidungsverhalten der Verbraucherinnen und Verbraucher maßgeblich beeinflussen.

In der verhaltenswissenschaftlichen Forschung beschreibt der Einrahmungseffekt (vgl. Tversky und Kahneman (1981)) wie das Verhalten von Verbraucherinnen und Verbrauchern auf unterschiedliche Art und Weise beeinflusst wird, wenn Inhalte und zugehörige Informationen unterschiedlich formuliert werden. Die International Association of Privacy Professionals (IAPP, 2017) nennt zwei Beispiele, die Einrahmungseffekte bei der Einwilligung verursachen und das Verhalten von Verbraucherinnen und Verbrauchern beeinflussen können. Diese können dafür verwendet werden, datensparsames Verhalten der Verbraucherinnen und Verbraucher zu fördern oder ein solches zu unterminieren:

i) Verwendung eines „Vertrauens-Frame“: Einwilligungen werden in der Realität oftmals über das Anklicken einer Schaltfläche gegeben. Hierbei werden z.B. (neutrale) „Zustimmen“- versus „Nicht zustimmen“-Schaltflächen genutzt. Eine weitere Möglichkeit, die Zustimmung einzuholen und dabei einen Einrahmungseffekt anzuwenden, wäre eine Umformulierung und das (Aus-)Nutzen eines Vertrauens-Frames. So könnte die Schaltfläche bspw. mit „Vertrauen“ und „Nicht Vertrauen“ beschriftet werden (vgl. Abbildung 1). Die verhaltenswissenschaftliche Literatur, insbesondere zu sozialen Normen, zeigt, dass diese Umformulierung die Einwilligungsrate insgesamt erhöhen kann, da das „Nicht Vertrauen“ subjektiv als falsches Verhalten gewertet werden könnte, während „Vertrauen“ der sozialen Norm entspricht.



Datenschutz
Hiermit erkläre ich mich mit den [Datenschutzbestimmungen](#) einverstanden.

Nicht Vertrauen Vertrauen

Abbildung 1: Beispiel für Vertrauens-Frame

ii) Verwendung eines „Experten-Frame“: Es ist bekannt, dass sich Verbraucherinnen und Verbraucher oftmals auf die Empfehlungen von Expertinnen und Experten verlassen und auf deren Einstellungen vertrauen. Im Gegensatz zu einer (neutralen) Formulierung wie „Zustimmen“ versus „Anpassen“ könnten die Schaltflächen bei der Einwilligung bspw. mit „Experteneinstellungen wählen“ versus „Anpassen“ versehen werden (vgl. Abbildung 2). Dies würde die Einwilligungsrate insgesamt erhöhen, da Verbraucherinnen und Verbraucher darauf vertrauen, dass Expertinnen und Experten wohl wissen, was in der Situation richtig ist.



Abbildung 2: Beispiel für Experten-Frame

Ein weiteres Beispiel für Framing wird im Gutachten des Büros für Technikfolgen-Abschätzung beim Bundestag hervorgehoben:

iii) Wechselnde Formulierungen: Ein weiterer Framing-Effekt, der dadurch zustande kommt, dass Nutzerinnen und Nutzer Informationen zum Teil nicht korrekt interpretieren, sind sog. wechselnde Formulierungen („Trickfragen“ vgl. Bogenstahl (2019)). Hierbei werden bspw. Aussagen in einer Entscheidungsstruktur abwechselnd mal bejahend und mal verneinend ausgedrückt (vgl. Abbildung 3). Lesen Nutzerinnen und Nutzer lediglich die erste Aussage und treffen dann alle Entscheidungen nach dem gleichen Muster, kann es sein, dass sie das veränderte Framing übersehen und Fehlentscheidungen treffen.

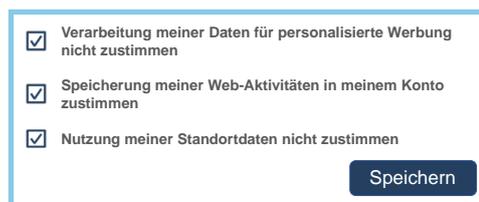


Abbildung 3: Beispiel für wechselnde Formulierungen

2.1.2.2.3. Voreinstellungen

Ein weiterer Aspekt, der bei der Einwilligung eine Rolle spielen kann, ist die Verwendung von Voreinstellungen, sog. Defaults. In der verhaltenswissenschaftlichen Literatur konnte gezeigt werden, dass Voreinstellungen die Entscheidungen von Verbraucherinnen und Verbrauchern maßgeblich beeinflussen.¹⁸³ So tendieren Verbraucherinnen und Verbraucher oftmals zu einer vorausgewählten Option, die für sie gesetzt wurde – auch wenn es prinzipiell möglich ist, eine andere Alternative auszuwählen.

Im Bereich der Einwilligung könnten Voreinstellungen für die Auswahl der Datenverarbeitung genutzt werden. Je nachdem welche Option vorausgewählt ist, wählen Verbraucherinnen und Verbraucher den Grad der Datenverarbeitung. Abbildung 4 zeigt beispielhaft die Umsetzung von Voreinstellungen bei der Datenerhebung.

¹⁸³ Für einen ausführlichen Überblick über Voreinstellungen und deren Wirkung auf das Verhalten von Verbraucherinnen und Verbrauchern siehe Kamenica (2012).

Standortdaten
Wir verarbeiten Ihre Standortdaten für kommerzielle Zwecke (Werbung). Ihre Standortdaten werden zu den gleichen Zwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weitergegeben und von diesen verarbeitet. Hierbei wird eine private Karte mit Orten, die Sie mit Ihren angemeldeten Geräten besuchen, erstellt, selbst wenn Sie gerade keines unserer Produkte nutzen.

Nutzung Standortdaten für kommerzielle Zwecke zustimmen

Nutzung Standortdaten für kommerzielle Zwecke nicht zustimmen

OK

Abbildung 4: Beispiel für Voreinstellungen

Voreinstellungen wirken sich dabei nicht nur auf die Entscheidung an sich, sondern auch auf die *Geschwindigkeit* der Einwilligung aus. Je schneller und einfacher es Verbraucherinnen und Verbrauchern gemacht wird, ihre Einwilligung umzusetzen, desto komfortabler.

Die Entscheidungsgeschwindigkeit kann demnach über die Voreinstellungen manipuliert werden und so nennen IAPP (2017) zwei Möglichkeiten der Gestaltung, die zu unterschiedlichen Entscheidungszeiten und Einwilligungsfrequenzen führen. Ist bspw. eine Voreinstellung gewählt und müssen Nutzerinnen und Nutzer lediglich durch Auswahl einer „Weiter“-Schaltfläche ein Fortfahren im Anmeldeprozess bestätigen, führt dies zu schnelleren und ggf. unüberlegten Entscheidungen. Im Gegensatz dazu forciert eine *Wahloption ohne Voreinstellung* das Pausieren und stärkere Verarbeiten der Informationen und somit eine Datenschutzentscheidung gemäß den eigenen Präferenzen (vgl. Abbildung 5).

Standortdaten
Wir verarbeiten Ihre Standortdaten für kommerzielle Zwecke (Werbung). Ihre Standortdaten werden zu den gleichen Zwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weitergegeben und von diesen verarbeitet. Hierbei wird eine private Karte mit Orten, die Sie mit Ihren angemeldeten Geräten besuchen, erstellt, selbst wenn Sie gerade keines unserer Produkte nutzen.

Nutzung Standortdaten für kommerzielle Zwecke zustimmen

Nutzung Standortdaten für kommerzielle Zwecke nicht zustimmen

OK

Abbildung 5: Beispiel für Wahloption ohne Voreinstellung (1/2)

Neben der Entscheidungsgeschwindigkeit spielt für die Wahloption ohne Voreinstellung auch ein weiterer Aspekt, nämlich die Anzahl der Auswahloptionen, eine maßgebliche Rolle. Während in den vorgestellten Beispielen lediglich zwei Auswahlmöglichkeiten präsentiert werden, ist es denkbar, dass eine Vielzahl von Optionen zur Auswahl gestellt wird. Die verhaltenswissenschaftliche Literatur weist jedoch darauf hin, dass es durch diese Vielzahl von Optionen zum sog. „Choice Overload“ kommen kann. So können mit einer steigenden Anzahl an Auswahloptionen nachteilige Konsequenzen einhergehen, die dazu führen, dass Verbraucherinnen und Verbraucher weniger motiviert sind, Entscheidungen zu treffen. Im ungünstigsten Fall kann dies dazu führen, dass Verbraucherinnen und Verbraucher aufgrund der Überlastung suboptimale Auswahlen treffen (Scheibehenne, 2010).

2.1.2.2.4. *Zugänglichkeit und Sichtbarkeit*

Des Weiteren spielen die Zugänglichkeit und Sichtbarkeit der Informationen und Differenzierungsmöglichkeiten eine Rolle für das Verständnis und Verbraucherverhalten in einer Einwilligungssituation. Nach Friedman (2004) wird dies im Modell der informierten Einwilligung unter der Voraussetzung *Agreement* (dt. Einigung und Zustimmung) subsumiert. Hierzu ist eine lesbare, zugängliche und sichtbare Möglichkeit zur Zustimmung von Nöten.

Kettner et al. (2018) zeigen auf, dass in diesem Zusammenhang der *Ort* der angezeigten Informationen relevant sein kann. So könnten Informationen hinter einem Link eingebunden werden und dadurch weniger sichtbar sein als wenn die Informationen immer im Hauptfenster angezeigt werden. Auch ist es möglich, Informationen oder Differenzierungsmöglichkeiten in einem auszuwählenden Pop-Up zu integrieren und so den Aufwand zum Erreichen der Informationen zu erhöhen. Je nachdem, an welchem Ort die Informationen und die Zustimmungsoptionen angezeigt werden, wird also beeinflusst, ob Verbraucherinnen und Verbraucher die Informationen tatsächlich wahrnehmen und verarbeiten und Einstellungen vornehmen.

Auch der *Zeitpunkt der Anzeige* der Informationen oder Einstellungsmöglichkeiten kann laut Kettner et al. (2018) die Einwilligung maßgeblich beeinflussen. Wenn datenschutzrelevante Informationen und Einstellungen am Ende eines Bestellprozesses, bspw. bei Online-Shopping, angezeigt werden, ist es möglich, dass die Einwilligung bereitwilliger gegeben wird, da man bereits weit im Einkaufsvorgang (Customer Journey) fortgeschritten ist und nun nicht mehr nach alternativen Angeboten suchen möchte.

2.1.2.2.5. *Gestaltung und Anordnung der Optionen*

Auch die Gestaltung der Informationen sowie die Anordnung der Auswahloptionen bei der Einwilligung spielt eine Rolle. Kettner et al. (2018) zeigen auf, dass die *Gestaltung* der begleitenden Einwilligungstexte bzw. Datenschutzerklärungen die Informiertheit der Verbraucherinnen und Verbraucher beeinflussen. Durch Zwischenüberschriften, Aufzählungslisten, Verbildlichungen oder eine Strukturierung der Texte in Cluster wird das Lesen und Verstehen unterstützt.

Bei der Präsentation der Alternativen, die bei einer Einwilligung angeboten werden können, weisen IAPP (2017) darauf hin, dass allein durch die Anordnung der Optionen die Auswahl der Verbraucherinnen und Verbraucher maßgeblich beeinflusst wird. So wählt die Mehrzahl der Verbraucherinnen und Verbraucher bei horizontaler Darstellung von zwei Optionen die rechte Option, während bei vertikaler Darstellung die Wahrscheinlichkeit für beide Optionen etwa gleich ist. Entsprechend kann die Gestaltung manipulativ zum Einsatz kommen.

2.1.2.2.6. *Ablenkung von wesentlichen Informationen*

Ein weiterer Aspekt, der in dem Modell der informierten Einwilligung von Friedman et al. (2005) berücksichtigt wird, ist *Minimal Distraction* (dt. minimale Ablenkung). So kann durch den Einsatz von zusätzlichen Informationen, die nicht zwingend mit der Einwilligung zu tun haben, dafür gesorgt werden, dass Verbraucherinnen und Verbraucher von den relevanten Inhalten abgelenkt werden.

Dieser Effekt kann auch durch den Einsatz von unterschiedlichen Schriftfarben und -größen erzielt werden. Ähnlich verhält es sich auch mit Fülltexten oder einem (künstlich) in die Länge gezogenen Anmeldeprozess (Bogenstahl, 2019). Somit ist aus verhaltenswissenschaftlicher Perspektive ein besonderes Augenmerk auf Ablenkungen zu richten.

2.1.2.2.7. *Inhaltliche Betrachtung*

Neben den eher gestalterischen Fragen einer Einwilligungsarchitektur, die bislang analysiert wurden, stellt sich auch die inhaltliche Frage, für welche Datenarten und Verarbeitungszwecke eine differenzierte Einwilligung insbesondere nötig ist.

In der Praxis ist die Anzahl der Differenzierungsdaten abhängig vom konkreten Geschäftsmodell und dem Angebot des Anbieters und man kann nicht pauschal vorfestlegen, für welche Datenarten und Verarbeitungszwecke differenziert werden muss und für welche nicht. Aus rechtlicher Perspektive ist außerdem eindeutig definiert, dass alle Verarbeitungsarten, die einer Einwilligung bedürfen, bei einer Differenzierung abgefragt werden müssen.

Abgeleitet aus dem PGuard-Forschungsprojekt¹⁸⁴, das mit Mitteln des Bundesministeriums für Bildung und Forschung umgesetzt wurde, lassen sich jedoch fünf übergeordnete und häufig genutzte Differenzierungstypen (sog. Cluster) definieren, die für Verbraucherinnen und Verbraucher eine besonders große Relevanz haben. Hierbei ist wichtig anzumerken, dass die Beschreibung der Differenzierungstypen lediglich eine neutrale Beschreibung darstellt – eine Bewertung ist an dieser Stelle nicht vorgesehen:

1. **Zugriff:** Hierunter wird der Zugriff von Anwendungen auf Webaktivitäten, den Standort, das Adressbuch oder von Sensoren verstanden.
2. **Identifikation:** Hierbei geht es um die Möglichkeit, Nutzerinnen und Nutzer sowie deren Geräte durch den Einsatz digitaler Technologien bei der wiederholten Nutzung von Webseiten oder Apps wiederzuerkennen.
3. **Profilbildung:** Dieser Verarbeitungszweck kann auf Grundlage unterschiedlicher personenbezogener Daten stattfinden. Es können Daten sein, die die Verbraucherinnen und Verbraucher selbst bewusst mitteilen (Name, E-Mail-Adresse etc.) oder es können Daten sein, die sich etwa aus der Nutzung eines Dienstes ergeben (Suchwörter, Nutzungsdauer etc.).
4. **Personalisierte Werbung:** Werbung, die auf Grundlage von Daten oder Profilen auf eine Person oder ein Gerät abgestimmt wurde, fällt unter den Begriff der personalisierten Werbung.
5. **Weitergabe an Dritte:** Die Weitergabe von Daten durch einen Anbieter an Dritte, bspw. andere Unternehmen, ist eine weitere Verarbeitungsart. Zu den Empfängern zählen bspw. Werbeanbieter, Cloud-Dienste oder soziale Medien, die in eine Webseite eingebunden werden.

¹⁸⁴ Kettner, S. E. et al. (2019). Privacy Guard - Abschlussbericht. Abgerufen von: <https://datenschutz-scanner.de/detail/news/forschungsprojekt-veroeffentlicht-gemeinsamen-abschlussbericht/> (09.03.2020)

Aus Verbraucherperspektive macht es oftmals einen Unterschied, welche der genannten Differenzierungstypen in einem Einwilligungsmodell angezeigt werden. Eine Befragung im Rahmen des PGuard-Forschungsprojekts liefert Anhaltspunkte, welche Datenverarbeitungen und Zwecke hierbei aus Sicht der Verbraucherinnen und Verbraucher eine besonders hohe Relevanz haben. Die konkrete Fragestellung war, wie wichtig es Verbraucherinnen und Verbrauchern zu erkennen ist, ob eine bestimmte Datenverarbeitung für einen bestimmten Zweck stattfindet oder nicht. „Erkennen“ kann sich dabei auf die Differenzierungsmöglichkeiten beziehen, d.h. einwilligungsrelevante Datenverarbeitungen, aber auch auf Datenverarbeitungen, die unter das berechnete Interesse fallen. Obwohl die Befragung nicht zwischen diesen beiden Typen (einwilligungsrelevant versus nicht) unterscheidet, ist die Bewertung der befragten Verbraucherinnen und Verbraucher dennoch ein Indikator für die Verbraucherinteressen. Abbildung 6 fasst die Bewertung der Differenzierungsmöglichkeiten zusammen.



Abbildung 6: Differenzierungsmöglichkeiten und Bewertung durch Verbraucherinnen und Verbraucher

Insgesamt ist zu erkennen, dass alle fünf Differenzierungsmöglichkeiten als sehr relevant von Verbraucherinnen und Verbrauchern bewertet werden. Nimmt man die Bewertungen „wichtig“ und „sehr wichtig“ zusammen, so ergeben sich Summen zwischen 76% und 83%. Zwischen den unterschiedlichen Differenzierungstypen gibt es im Hinblick auf eine sehr hohe Relevanzbewertung („sehr wichtig“) jedoch Unterschiede. So gibt bei der Weitergabe an Dritte die Mehrheit von 54% an, dass es ihnen sehr wichtig ist, zu erkennen, ob eine solche Verarbeitung stattfindet. Ähnlich hoch – mit 52% „sehr wichtig“ – ist die Bewertung des Verarbeitungszweckes Identifikation. Profilbildung und Zugriff erhalten immerhin 45% bzw. 42% Zustimmung für die sehr hohe Relevanz. Personalisierte Werbung wird ebenfalls als „sehr wichtig“ erachtet, jedoch lediglich von einem Anteil von 38% der Befragten.

Zusammenfassend lässt sich also feststellen, dass alle fünf genannten Datenverarbeitungen und -zwecke für die Differenzierung bei Verbraucherinnen und Verbrauchern eine große Rolle spielen. Wenn also innerhalb des Angebots keine Erforderlichkeit nach berechtigtem Interesse vorliegt, sind dies auch die relevanten Aspekte, über die ein Einwilligungsmodell differenzieren sollte. Im theoretischen Best Practice-Modell, das im Rahmen der zugrundeliegenden Studie entwickelt werden soll, werden deshalb die fünf genannten Differenzierungstypen vollständig berücksichtigt.

2.1.2.2.8. *Zwischenfazit: Das Einwilligungsverhalten der Verbraucherinnen und Verbraucher kann durch die Einwilligungsarchitektur in unterschiedlichster Weise beeinflusst werden*

Wie die Zusammenfassung der verhaltenswissenschaftlichen Erkenntnisse zeigt, kann das Einwilligungsverhalten der Verbraucherinnen und Verbraucher durch die Gestaltung der „Einwilligungsarchitektur“ beeinflusst werden. Diese Einwilligungsarchitektur kann so ausgestaltet werden, dass es Verbraucherinnen und Verbrauchern möglichst einfach gemacht wird, informierte und ihren Präferenzen entsprechende Entscheidungen zu treffen. Sie kann aber auch so ausgestaltet werden, dass das Verbraucherverhalten in die Richtung manipuliert wird, dass Verbraucherinnen und Verbraucher möglichst umfangreiche Einwilligungen erteilen und sie auch nur umständlich ändern können (siehe hierzu u.a. auch eine Veröffentlichung der norwegischen Verbraucherorganisation Forbruker Radet¹⁸⁵).

Wie dieser Abschnitt zeigt, zählen zu den wesentlichen Faktoren, die eine Einwilligungsarchitektur charakterisieren:

- die Aufbereitung der Informationen und Texte,
- das Framing der Entscheidungssituation,
- die Art der Einwilligung (mit oder ohne Voreinstellungen),
- die Zugänglichkeit und Sichtbarkeit,
- die Gestaltung und Anordnung der Optionen sowie
- die Ablenkung von wesentlichen Informationen.

Überdies zeigt die inhaltliche Betrachtung, dass Verbraucherinnen und Verbraucher insgesamt ein hohes Interesse dafür haben, zwischen den folgenden Datenverarbeitungen differenziert einwilligen zu können: Weitergabe an Dritte, Identifikation, Profilbildung, Zugriff und personalisierte Werbung.

2.2. Einwilligungsmanagementmodelle aus Praxis und Theorie

Im Folgenden werden ausgewählte Einwilligungsmodelle vorgestellt und deren Nutzerführungskonzepte sowie Einzelfunktionen beschrieben. Zunächst wird auf Einwilligungssysteme von Einzelanbietern aus der Praxis eingegangen. Danach werden Vorschläge aus der Wissenschaft, d.h. theoretische Systeme, und dann übergreifende Einwilligungssysteme vorgestellt. Zum Abschluss folgen sonstige Erkenntnisse etwa über die Gestaltung von Einwilligungsmanagementssystemen in mobilen Umgebungen und sonstige nennenswerte Funktionen, die die Einwilligungsarchitektur auszeichnen.

2.2.1. Praxisbeispiele für die Einwilligung bei Einzelanbietern

Allgemein unterscheiden sich die folgenden Beispiele zur Einwilligung bei Einzelanbietern vor allem im Grad der Differenzierung bzw. der Möglichkeit, Einwilligungen für unterschiedliche Datenarten und Zwecke spezifisch zu erteilen. Die

¹⁸⁵ Forbruker Radet. (2018). Deceived by design. Abgerufen von <https://www.forbrukerradet.no/undersokelse/nundersokelsekategori/deceived-by-design/> (22.08.2019)

überwiegende Mehrheit der von uns identifizierten Anbieter lässt sich *globale Einwilligungen* in impliziter oder expliziter Form geben. Wir konnten nur sehr wenige Praxisbeispiele finden, in denen Verbraucherinnen und Verbraucher differenzierte Einwilligungen für einzelne Datenarten und Zwecke erteilen können.

Im Folgenden gehen wir zunächst auf *globale Einwilligungssysteme*, dann auf *differenzierte Einwilligungssysteme* und im Anschluss auf solche Systeme ein, mit denen *Einwilligungen im Nachhinein* verändert werden können.

2.2.1.1. Globale Einwilligung durch Bestätigung

Die überwiegende Mehrheit der untersuchten Unternehmen nutzt im Anmeldeprozess, d.h. in der Customer Journey etwa zum Anlegen eines Nutzerkontos, den Weg der *globalen Einwilligung*. Hierbei werden Nutzerinnen und Nutzer gebeten, allen Datenverarbeitungen auf einmal zuzustimmen.

In manchen Fällen wird in einem zusammenfassenden Text darauf hingewiesen, dass der Klick der „Registrieren“-Schaltfläche einer Zustimmung zur Datenverarbeitung entspricht.

„Indem du dich registrierst, stimmst du den Allgemeinen Geschäftsbedingungen und den Datenschutzrichtlinien [...] zu“ (Beispiel 1 aus dem Anmeldeprozess zu einem sozialen Netzwerk)

Hier werden die Informationen zur Datenverarbeitung zumeist hinter einem Link eingebunden und sind über einen neuen Tab zu erreichen.

In anderen Fällen ist eine *aktive Einwilligung* vorgesehen, bei der eine Check-Box angeklickt oder ein Haken gesetzt werden muss, der die Einwilligung explizit macht.

„Ja, ich stimme den AGB und Datenschutzbestimmungen [...] zu.“
(Beispiel 2 aus dem Anmeldeprozess eines Online-Shops)

Wird die explizite Zustimmung im Anmeldeprozess nicht gegeben, d.h. die Check-Box nicht angeklickt, kann der Anmeldeprozess nicht abgeschlossen werden. Die Einwilligung ist dabei oftmals als Pflichtfeld markiert.

Eine weitere Umsetzung der aktiven Einwilligung findet sich in Einzelfällen auch für bestimmte, gesonderte Datenverarbeitungen. Hierbei wird nicht global der Datenverarbeitung zugestimmt, da diese sich bspw. auf das berechtigte Interesse bezieht, sondern es wird eine Einwilligung zur Datenverarbeitung für einen Newsletter oder weitere Marketingmaßnahmen eingeholt.¹⁸⁶ Auch hier muss zum Abschließen des Anmeldeprozesses eine Check-Box angeklickt oder ein Haken gesetzt werden. Ohne die aktive Einwilligung ist ein Abschluss nicht möglich.

„Ich möchte zukünftig über [...] Aktionen und Angebote [...] informiert werden. Diese Einwilligung kann jederzeit [...] widerrufen werden.“
(Beispiel 3 aus dem Anmeldeprozess eines Online-Shops)

¹⁸⁶ Da es sich in diesem Fall um eine Zustimmung zu Werbeaktivitäten nach §7 Abs. 2 Nr. 3 UWG handelt, ist aktuell noch umstritten, ob die DS-GVO oder die künftige ePrivacy-Richtlinie Anwendung finden wird.

Auch wenn die Einwilligung zumeist an Werbeaktivitäten des Anbieters gebunden ist, kann man bei strikter Auslegung von einer erzwungenen Einwilligung sprechen, insbesondere, wenn keine Alternativen zum Anlegen eines Kontos ohne die genannte Verarbeitung möglich sind.

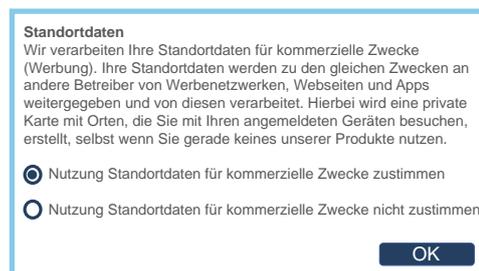
2.2.1.2. Differenzierte Einwilligung

Neben der globalen Einwilligung findet sich bei einigen wenigen Anbietern die Möglichkeit, zwischen unterschiedlichen Verarbeitungszwecken und Datenarten in der Einwilligung zu differenzieren. Hierbei können Verbraucherinnen und Verbraucher auswählen, ob sie möchten, dass bestimmte Datenverarbeitungen zu ausgewählten Zwecken vorgenommen werden oder nicht. Die Bandbreite der Differenzierung reicht dabei von der Erhebung von Standortdaten oder des Nutzungsverhaltens bis hin zur personalisierten Werbung.

Diese unterschiedlichen Differenzierungsarten werden im Folgenden beschrieben. Zwar sind diese Umsetzungen der Differenzierung in der Praxis rar, jedoch sollten (zumindest theoretisch) zwei Ausgestaltungen der Differenzierungsoptionen unterschieden werden. Die erste ist die mit vorausgewählten Voreinstellungen. Sie findet sich in der Praxis bei zwei von uns untersuchten Unternehmen. Die zweite ist die Wahloption ohne Voreinstellung, die in keinem relevanten Praxismodell zu finden ist. Beide werden im Folgenden mit Blick auf die Nutzerführung beschrieben.

2.2.1.2.1. Voreinstellungen vorausgewählt

Sofern Differenzierungsmöglichkeiten derzeit von den Unternehmen, die wir betrachtet haben, angeboten werden, handelt es sich um Modelle, bei denen eine Verarbeitung bereits vorausgewählt ist (vgl. Abbildung 7). So werden bspw. Datenverarbeitungen per Voreinstellung ausgewählt und Nutzerinnen und Nutzer können durch einen Klick die andere Option auswählen, bei der die Daten nicht verarbeitet werden.



The image shows a dialog box titled "Standortdaten". The text inside reads: "Wir verarbeiten Ihre Standortdaten für kommerzielle Zwecke (Werbung). Ihre Standortdaten werden zu den gleichen Zwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weitergegeben und von diesen verarbeitet. Hierbei wird eine private Karte mit Orten, die Sie mit Ihren angemeldeten Geräten besuchen, erstellt, selbst wenn Sie gerade keines unserer Produkte nutzen." Below the text are two radio button options: "Nutzung Standortdaten für kommerzielle Zwecke zustimmen" (which is selected) and "Nutzung Standortdaten für kommerzielle Zwecke nicht zustimmen". An "OK" button is located at the bottom right of the dialog.

Abbildung 7: Beispiel für voreingestellte Datenverarbeitung mit Knöpfen („zugestimmt“)

Ein Beispiel für ein solches Modell mit Voreinstellungen ist der Anmeldeprozess für ein Google-Konto mit zugehöriger Gmail-Adresse. Hierbei tragen Nutzerinnen und Nutzer im ersten Schritt des Anmeldeprozesses ihren Namen, ihren Nutzernamen und das Passwort ein. Die Datenschutzerklärung ist im unteren Bereich der Seite verlinkt. Im zweiten Schritt können Nutzerinnen und Nutzer weitere z.T. optionale Daten, wie Telefonnummer, Geburtsdatum und Geschlecht eingeben. Speziell für diese Datenarten wird eine Erläuterung verlinkt, in der nachzulesen ist, wofür die Daten erhoben werden. Im dritten Schritt wer-

den unter dem Titel „Datenschutz und Bedingungen“ Informationen zur Datenverarbeitung angeboten. So wird u.a. die Datenschutzerklärung bzw. deren Inhalte verlinkt und zu den relevanten Datenverarbeitungsarten und Zwecken eine kurze Zusammenfassung als Spiegelstriche angezeigt. Darunter findet sich die Möglichkeit, durch Check-Boxen zuzustimmen. Bis zu diesem Punkt unterscheidet sich das Google-Modell also nicht von anderen Modellen, die untersucht wurden und bspw. in die Kategorie der globalen Einwilligung fallen. Doch findet sich neben der direkten, undifferenzierten Zustimmungsmöglichkeit auch die Option („Weitere Optionen“), Datenarten und Verarbeitungszwecke zu differenzieren.

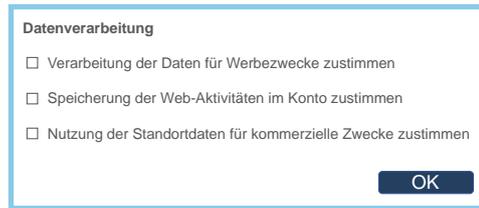
Abbildung 8 zeigt die Ausgestaltung des Bereichs „Weitere Optionen“, in dem die Differenzierung über insgesamt sechs Verarbeitungsarten bzw. Zwecke ermöglicht wird. Hierzu zählen (1) Web- und App-Aktivitäten, (2) Personalisierte Werbung, (3) YouTube-Suchverlauf, (4) YouTube-Wiedergabeverlauf, (5) Standortverlauf sowie (6) Sprach- und Audioaktivitäten. Die ersten vier Differenzierungsmöglichkeiten sind dabei voreingestellt, d.h. die Zustimmung der Verarbeitung ist vorausgewählt und der obere der beiden Auswahl-Buttons ist demnach angeklickt. Nutzerinnen und Nutzer müssten durch Klicken auf den unteren Auswahl-Button die Einstellung abändern (Opt-Out). Die letzten beiden Differenzierungsmöglichkeiten sind hingegen datensparsam voreingestellt. Sollten Verbraucherinnen und Verbraucher die jeweiligen Datenverarbeitungen wünschen, müssten sie durch Klicken die Voreinstellung anpassen (Opt-In).

Alle Differenzierungsoptionen werden durch einen kurzen, begleitenden Text beschrieben. Wenn Nutzerinnen und Nutzer zusätzliche Informationen zur Verarbeitung wünschen, ist es möglich, über den Link „Weitere Informationen“ ein Pop-Up aufzurufen, in dem die Datenverarbeitungen und -zwecke detaillierter beschrieben werden.



Abbildung 8: Beispiel für voreingestellte Datenverarbeitungen mit Buttons (Google)

Eine andere Ausgestaltung des Modells mit Voreinstellung findet in der Praxis ebenfalls Anwendung. Bei diesem werden alle differenzierten Datenverarbeitungen untereinander aufgelistet und mit Check-Boxen versehen (vgl. Abbildung 9). Wenn Nutzerinnen und Nutzer eine Verarbeitung wünschen, können sie die Check-Box anklicken und einer Verarbeitung zustimmen. Die Voreinstellung ist das Nichterheben der Daten und ein Fortfahren im Anmeldeprozess ist auch ohne Auswahl möglich.



Datenverarbeitung

- Verarbeitung der Daten für Werbezwecke zustimmen
- Speicherung der Web-Aktivitäten im Konto zustimmen
- Nutzung der Standortdaten für kommerzielle Zwecke zustimmen

OK

Abbildung 9: Beispiel für voreingestellte Datenverarbeitung mit Check-Boxen ("nicht zugestimmt")

Ein Beispiel für die Umsetzung eines solchen Modells in der Praxis findet sich beim Anlegen eines Nutzer-Accounts für die Plattform openSAP (vgl. Abbildung 10). Im Gegensatz zum Google-Modell werden alle Einstellungsmöglichkeiten auf einer Seite präsentiert und Nutzerinnen und Nutzer müssen – je nach Darstellung ihres Endgeräts – durch die Seite scrollen. Vor den relevanten Datenfeldern wird die Datenschutzerklärung sichtbar verlinkt. Danach können Nutzerinnen und Nutzer ihren Namen, ihre E-Mail-Adresse und das Passwort eingeben. Hierunter finden sich die Differenzierungsmöglichkeiten mit Check-Boxen, die nicht voreingestellt und angeklickt sind. D.h. Nutzerinnen und Nutzer, die einer Datenverarbeitung zustimmen möchten, klicken die Check-Box an, während die, die einer Datenverarbeitung nicht zustimmen möchten, die Voreinstellung unverändert lassen.

Insgesamt sieht das Modell neben dem erforderlichen Anlegen eines Benutzerprofils drei relevante Differenzierungen vor. Zu denen zählen das (1) Web-Tracking, (2) Marketing (Werbung) und (3) Angebote für Partner.

Registrieren

Legen Sie Ihren eigenen Account bei openSAP an. Dazu müssen Sie nur wenige Angaben machen.
Ihr Name wird später auf Ihrem openSAP-Zeugnis erscheinen.

Bitte beachten Sie: Ihre personenbezogenen Daten werden auf openSAP unter den Bedingungen unserer **Datenschutzbestimmungen** verarbeitet. Mit der Registrierung eines Benutzerkontos auf openSAP erkennen Sie diese **Datenschutzbestimmungen** an.

* Ihr Vorname

* Ihr Nachname

* Ihre E-Mail-Adresse

* Passwort

* Passwort (Wiederholung)

Benutzerprofil **Verpflichtend**

Ich erlaube, dass openSAP das von mir angegebene Benutzerprofil speichert. Teile des Profils können von anderen Nutzern der Plattform in Diskussionsforen oder anderen kollaborativen Funktionen eingesehen werden. Dies umfasst den **Klarnamen**, sofern kein expliziter **Anzeigename** gesetzt wird, sowie ein optionales Profilfoto.

Web Tracking

Ich erlaube, dass openSAP Statistiken über meine Nutzung des Angebots speichern und zu Zwecken der Förderung meiner Lernerfahrung und Verbesserung des openSAP-Angebots auswerten darf. Die Speicherung erfolgt anonym.

Marketing

Ich erlaube, dass openSAP mich via E-Mail über folgende Themen informiert

- Kursverwandte Angebote und Dienstleistungen, wie Rabatte von openSAP Reactivation Codes, SAP Learning Hub Abonnements und weitere Materialien und Empfehlungen außerhalb der openSAP Plattform
- Kommunikation basierend auf meinen Präferenzen und meiner Lernhistorie, wie spezielle Angebote für herausragende Kursleistungen

Jegliche Kommunikation geht direkt von openSAP aus und meine personenbezogenen Daten werden nicht mit einer anderen Organisation innerhalb oder außerhalb von SAP geteilt.

Abbildung 10: Beispiel für voreingestellte Datenverarbeitung mit Check-Boxen (openSAP)

2.2.1.2.2. Wahloption ohne Voreinstellung

Die zweite Möglichkeit, Verbraucherinnen und Verbraucher differenziert einwilligen zu lassen, ist die Wahloption ohne Voreinstellung. Sie findet sich in der Praxis in keinem der von uns untersuchten Modelle und wird deshalb im Folgenden lediglich theoretisch beschrieben. So würde der Anbieter Differenzierungsoptionen anbieten und die Nutzerinnen und Nutzer auffordern, aktiv auszuwählen, ob sie eine Datenverarbeitung wünschen oder nicht. Die Nutzerinnen und Nutzer müssen sich zwischen den Optionen entscheiden, sonst kommen sie im Anmeldeprozess (Customer Journey) nicht weiter. Somit ist weder die Verarbeitung noch die Nichtverarbeitung vorausgewählt und die Präferenzen müssen explizit geäußert werden. Abbildung 11 zeigt dies an einem Beispiel.



The image shows a dialog box titled "Standortdaten" (Location Data). The text inside reads: "Wir verarbeiten Ihre Standortdaten für kommerzielle Zwecke (Werbung). Ihre Standortdaten werden zu den gleichen Zwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weitergegeben und von diesen verarbeitet. Hierbei wird eine private Karte mit Orten, die Sie mit Ihren angemeldeten Geräten besuchen, erstellt, selbst wenn Sie gerade keines unserer Produkte nutzen." Below the text are two radio button options: "Nutzung Standortdaten für kommerzielle Zwecke zustimmen" (selected) and "Nutzung Standortdaten für kommerzielle Zwecke nicht zustimmen". At the bottom right is an "OK" button.

Abbildung 11: Beispiel für eine Wahloption ohne Voreinstellung (2/2)

Nutzerinnen und Nutzer haben dabei die Möglichkeit, der Erhebung von Standortdaten zuzustimmen (Wahl des ersten, oberen Buttons) oder abzulehnen (Wahl des zweiten, unteren Buttons). Ein Fortfahren im Anmeldeprozess ist dabei erst möglich, wenn eine explizite Entscheidung getroffen wurde.

2.2.1.3. Einwilligungsmangement im Nachhinein

Die bisher vorgestellten Beispiele für Einwilligungssysteme sind alle in einen Anmeldeprozess integriert. Das bedeutet, dass die Einstellungen *vor der Datenerhebung* vorgenommen werden und Nutzerinnen und Nutzer ihre Präferenzen im Anmeldeprozess zum Ausdruck bringen müssen.

Eine weitere Variante zur Verwaltung von Einwilligungen, die in der Praxis zu finden ist, ist das Einwilligungsmangement im Nachhinein. Hierbei wird es Nutzerinnen und Nutzern ermöglicht, ihre Datenschutzeinstellungen bspw. über ein Portal, Cockpit oder Dashboard vorzunehmen. Die Ausgestaltungen und Nutzeroberflächen sind dabei anbieterabhängig und in den Fällen, in denen eine differenzierte Einwilligung bei der Anmeldung vorgenommen werden kann, spiegelt das System die Einwilligungsfunktionen und Gestaltungsparameter wider.

Es gibt jedoch auch Praxisbeispiele, die bei der Einwilligung im Anmeldeprozess eine globale Einwilligung einholen und über ein gesondertes Portal oder Dashboard erst im Nachhinein ermöglichen, Datenverarbeitungen zu deaktivieren (Widerruf der Einwilligung).

Das bekannteste Beispiel für ein Einwilligungsmangement im Nachhinein innerhalb eines Nutzerkontos ist Google My Account. In diesem können Daten eingesehen und angepasst werden und in einem gesonderten Bereich „Daten & Personalisierung“ können Privatsphäreinstellungen getätigt werden. Selbiges ist im Bereich „Privatsphärecheck“ möglich, in dem Nutzerinnen und Nutzer die personalisierbaren Zwecke und Datenarten einstellen können.

Im Google My Account können die oben bereits beschriebenen Differenzierungsarten (1) Web- und App-Aktivitäten, (2) Personalisierte Werbung, (3) YouTube-Suchverlauf, (4) YouTube-Wiedergabeverlauf, (5) Standortverlauf sowie (6) Sprach- und Audioaktivitäten im Bereich der „Aktivitätseinstellungen“ eingesehen werden.

Abbildung 12 zeigt eine Übersicht über die gewählten Einstellungen. Dabei sind alle Datenverarbeitungen „Pausiert“, d.h. nicht aktiv. Wenn Nutzerinnen und Nutzer Anpassungen an den Einstellungen vornehmen möchten, können Sie dies über eine Auswahl in der Übersicht tun.

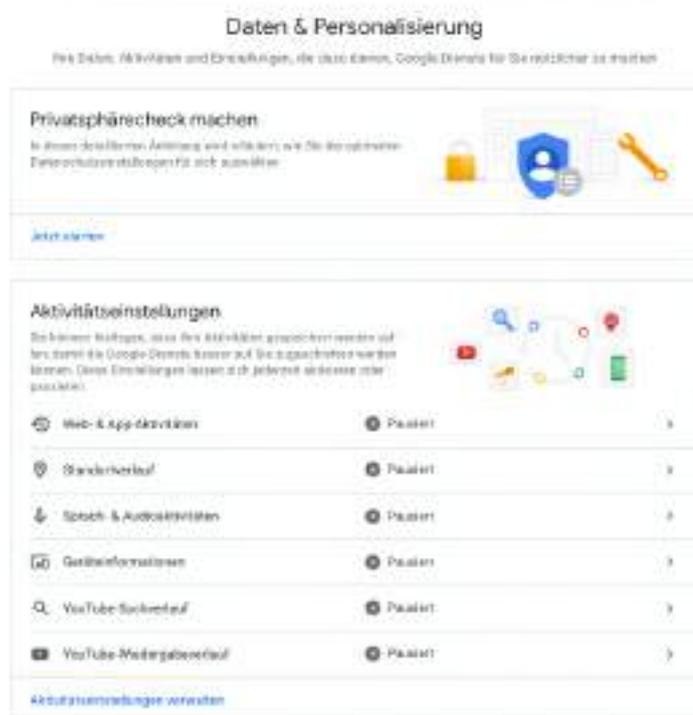


Abbildung 12: Beispiel für Einwilligungsmanagement im Nachhinein (1/2) (Google My Account)

Eine weitere Möglichkeit, Anpassungen an den selbstgewählten Datenverarbeitungen vorzunehmen, findet sich im Bereich „Privatsphärecheck“ (vgl. Abbildung 13). Auch hier werden parallel zum Anmeldeprozess die Datenarten nacheinander aufgelistet und die Einstellungen können gemäß den eigenen Präferenzen angepasst werden. Im Gegensatz zur Übersicht in den „Aktivitätseinstellungen“ werden alle Datenverarbeitungsarten und Zwecke überblicksartig beschrieben und weitere Erläuterungen verlinkt. So können sich Nutzerinnen und Nutzer im Detail informieren, für welche Zwecke ihre Daten verarbeitet werden und welchen Nutzen sie hieraus ziehen können.



Abbildung 13: Beispiel für Einwilligungsmanagement im Nachhinein (2/2) (Google My Account)

2.2.2. Beispiele aus der Theorie

In der Literatur finden sich weitere (theoretische) Beispiele, in denen Einwilligungsmanagementsysteme skizziert werden. Einige von ihnen sollen Nutzerinnen und Nutzern perspektivisch sogar ermöglichen, globale Einstellungen für mehrere Dienste vorzunehmen und die Daten in übergeordneten Portalen zu verwalten. Es ist jedoch wichtig anzumerken, dass die Beispiele aus diesen wissenschaftlichen Publikationen noch nicht genutzt werden können und manche Funktionen noch nicht ausdefiniert sind. Deshalb ist eine ausführliche Beschreibung, wie sie bei den Praxisbeispielen vorgenommen wurde, nicht möglich.

2.2.2.1. Differenzierte Einwilligung

Das *Layered Privacy Language Personal Privacy Policy User Interface (LPL PPP UI)* der Universität Passau hat eine Spezifikation für eine Nutzeroberfläche entwickelt, die Nutzerinnen und Nutzer über Datenverarbeitungen informieren und eine Personalisierung der Einwilligung ermöglichen soll (Gerl & Prey, 2018). Innerhalb der Oberfläche sollen Nutzerinnen und Nutzer für unterschiedliche Zwecke, d.h. (1) Statistik, (2) Forschung, (3) öffentlichen Zugang und (4) Datenübertragung sowie unterschiedliche Empfänger der Daten zustimmen oder diese ablehnen können. Welche genauen inhaltlichen Datenverarbeitungen und Zwecke hierbei vorgesehen werden, geht aus dem Demonstrator aufgrund seines hypothetischen Charakters nicht hervor.

Abbildung 14 zeigt die beispielhafte Darstellung für die Datenverarbeitung eines einzelnen Anbieters innerhalb der LPL PPP-Nutzeroberfläche. Im Bereich „Purpose Overview“ können Nutzerinnen und Nutzer ihre Daten für einzelne Zwecke wie bspw. Forschung freigeben. Dabei sind Check-Boxen vorgesehen, die angeklickt werden können, wenn Nutzerinnen und Nutzer der Verarbeitung zustimmen möchten. Darüber hinaus erhalten sie Informationen über die notwendigen Datenverarbeitungen in einer Detail-Ansicht. Hier wird erläutert, welche Daten tatsächlich für den genannten Zweck verwendet werden, wer die Daten erhält, wie lange die Daten gespeichert werden und welche Anonymisierungsverfahren vorgesehen sind.

Die Oberfläche steht Verbraucherinnen und Verbrauchern nicht im Rahmen einer realen Anwendung zur Verfügung, wurde jedoch bereits in einer kleinen experimentellen Studie mit Fokus auf die Verständlichkeit der Informationen an Probanden getestet. Jedoch sind die Fallzahlen sehr gering (N=12), so dass keine Rückschlüsse auf die Wirksamkeit gemacht werden können. Darüber hinaus wurden die Einstellungsmöglichkeiten der Datenverarbeitungen nicht getestet, so dass unklar bleibt, wie das System auf Nutzerinnen und Nutzer wirkt.

The screenshot displays a web interface for a Privacy Policy (PPP) with a 'Policy Header' and a 'Legal Privacy Policy' link. The main navigation bar includes 'Statistics', 'Research', 'Public Access', and 'Data Transfer'. The 'Purpose Overview' section on the left lists 'Research' as a selected purpose, with sub-options for 'Publishing of Result', 'Statistics', and 'Assessment', each with a 'required?' status. The 'Purpose Detail' section for 'Research' provides the following information:

- Which data is used and how?**
 - Personal Data:** Prenom, Surname, Funtel Num., Creation Date.
 - Personal Data:** Prenom, Surname of Applicant, Anonymisierungsverfahren: Suppression, Description: Removal of Characters.
 - Data Anonymity:** Technique 1, Technique 2, Technique 3, Technique 4, Technique 5.
- Who is the receiver of my data?**
 - University of Tübingen; University of Tübingen is a research facility.
- How long will my data be saved?**
 - Delete after research:** Data will be deleted after it is no longer necessary for the research within the DfG's project. Retention date: 03.07.2019.
- How secure will my data be anonymized?**
 - Anonymity:** At least 3 records with the same ID will exist so a de-anonymization risk of 10 is applied. With what probability I can be identified if an anonymized dataset: 33,33%.
 - K. ANONYMITÄT: 3; 3**
 - K. ANONYMITÄT: MAX. OUTLIERS: 0/02**

Abbildung 14: Demonstrator des LPL PPP UI-Modells (Gerl & Prey, 2018)

Ein weiteres theoretisches Modell, das in einem Forschungsprojekt an der TU Berlin entwickelt wurde, ist das *Einwilligungsmanagement für das Internet der Dinge (EMIDD)* von Ulbricht und Pallas (2018). Ziel des Projekts war die Entwicklung eines technischen Konzepts und einer Anwendung, mit der Verbraucherinnen und Verbraucher differenzierte Einwilligungen für Daten im Internet der Dinge verwalten können. Abbildung 15 zeigt Prototypen des Systems, das jedoch ebenfalls nicht für Verbraucherinnen und Verbraucher in realen Anwendungen zugänglich ist.

Auf der linken Seite der Abbildung findet sich die Nutzeroberfläche, die zusammenfasst, für welche Zwecke und Empfänger eine Datenverarbeitung erlaubt oder ausgeschlossen ist. Hierbei unterscheidet das Modell zwischen kommerziellen und nicht-kommerziellen Zwecken und sieht eine sehr feingliedrige Unterteilung an Verwendern, wie bspw. NGOs, öffentlichen Institutionen und Wirtschaftsunternehmen vor. Nutzerinnen und Nutzer können zusätzliche Zwecke und Verwender durch Eingabe in ein Textfeld ergänzen. Weiterhin sind detaillierte Informationen über ein Text-Overlay zugänglich. Die rechte Seite der Abbildung zeigt die App-Oberfläche, die die Spezifikation von Einwilligungen mobil ermöglichen soll. Auch hier wird zwischen unterschiedlichen Verwendergruppen unterschieden und diese können einzeln hinzugefügt oder entfernt werden. Darüber hinaus werden Nutzerinnen und Nutzern bei Bedarf Detailinformationen in kleinen Pop-Up-Fenstern eingeblendet.

Im Fall des EMIDD-Forschungsprojekts wurde keine Wirksamkeitsmessung an Nutzerinnen und Nutzern vorgenommen, deshalb ist unklar, ob und wie Verbraucherinnen und Verbraucher das Modell in der Realität verwenden würden.

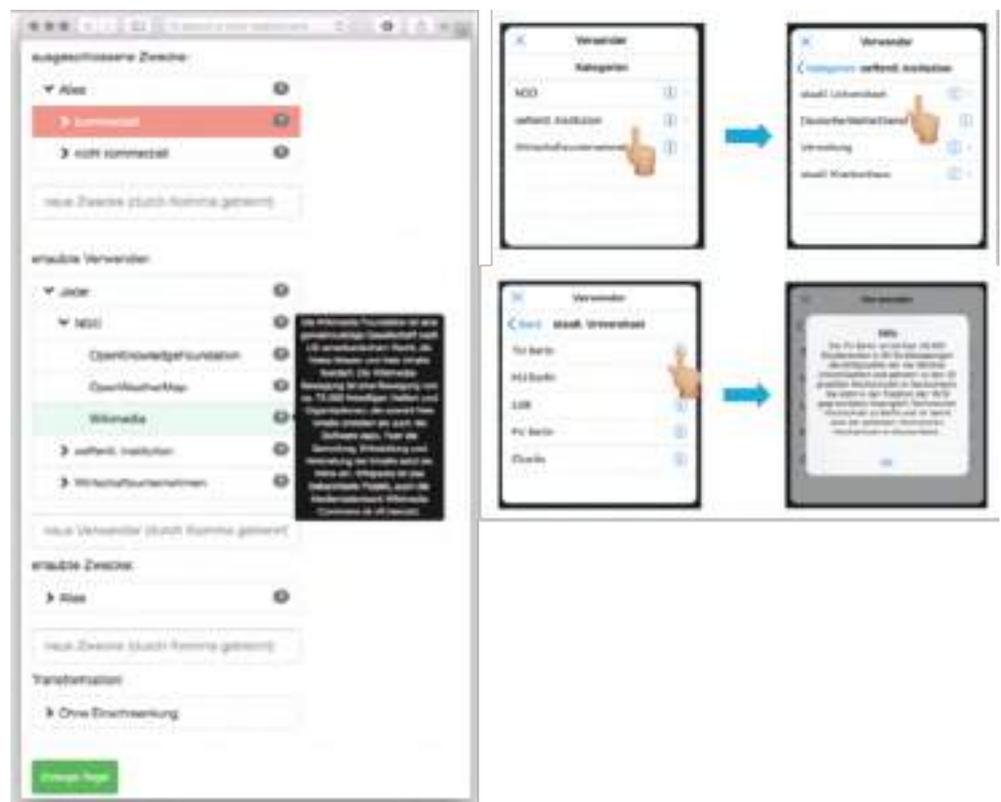


Abbildung 15: Demonstrator des EMIDD-Modells (Ulbricht & Pallas, 2018)

Im Forschungsprojekt *SPECIAL* (Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance), das durch die Europäische Union gefördert wird, werden unter anderem Lösungen entwickelt, mit denen Nutzerinnen und Nutzer ihre Einwilligungen verwalten können. Im Projekt sind bisher mehrere Prototypen für Nutzeroberflächen entstanden. Auffällig bei allen Prototypen ist, dass sehr ausführliche Tutorials und Hilfestellungen zur Erläuterung der Nutzerführung eingesetzt werden.

Abbildung 16 zeigt den *Consent and control UI prototype 2*, mit dessen Hilfe die Funktionen eines Fitnesstrackers und zugehörige Datenverarbeitungen personalisiert werden können. Insgesamt können Nutzerinnen und Nutzer über elf unterschiedliche Funktionen wie Frequenzmessung, gezielte Fitnesswerbung und Datensicherung entscheiden. Für jede Funktion wird dabei in einer Grafik visualisiert, welche Daten gespeichert und verarbeitet werden. So wird auch darüber informiert, ob die Verarbeitung auf dem Gerät stattfindet oder eine Weitergabe an Dritte vorgesehen ist. Über eine Schaltfläche werden die Funktionen und Verarbeitungsarten akzeptiert bzw. widerrufen. Im letzten Schritt können sich Nutzerinnen und Nutzer eine Zusammenfassung der zugestimmten Datenarten anzeigen lassen. Je nach Menge der Verarbeitungsarten kann diese Übersicht jedoch sehr schnell unübersichtlich werden.

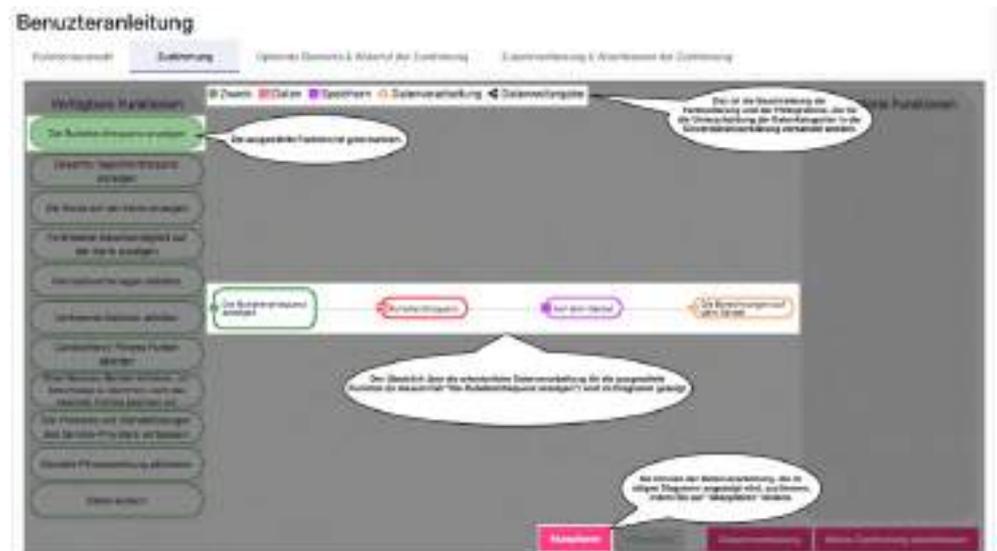


Abbildung 16: Demonstrator des SPECIAL Consent and control 2-Modells (SPECIAL, 2018)

Auch der *Consent and control UI prototype 3* ermöglicht Nutzerinnen und Nutzern, ihre Einwilligungen granular zu personalisieren und geht dabei auf die unterschiedlichen Zwecke der Datenverarbeitungen ein (Drozd & Kirrane, o. D.). Abbildung 17 zeigt den Demonstrator, der ebenfalls für das Nutzungsszenario eines Fitnesstrackers konzipiert ist. Auch in diesem Modell können Nutzerinnen und Nutzer differenziert über elf Funktionen entscheiden und differenziert angeben, ob sie einer Verarbeitung für diesen Zweck zustimmen. Vorgelagert zu den elf Funktionen findet sich jedoch eine Unterteilung der Verarbeitungsarten in (1) keine Funktionalität, d.h. keine Datenverarbeitung, (2) Gesundheitsdaten, (3) Kartenvisualisierung, (4) Fitnessempfehlungen, (5) Speicherung bis hin zu (6) Marketing und Business Intelligence, bei der alle möglichen Verarbeitungsarten akzeptiert sind. Über einen Schieberegler können Nutzerinnen und Nutzer den

Umfang dieser übergeordneten Datenverarbeitungen einstellen. Zusätzliche Informationen zu den Verarbeitungen sind über Text-Overlays eingebunden. Auch in diesem Prototyp sind Zusammenfassungen vorgesehen.

In einer Evaluation konnten die Autorinnen zeigen, dass die Anwendung einfach und verständlich möglich ist, jedoch ist unklar, wie sie auf eine breitere Nutzergruppe wirkt und ob die Bedienung nutzerfreundlich ist.



Abbildung 17: Demonstrator des SPECIAL Consent and control 3-Modells (Drozd & Kirrane, o.D.)

2.2.3. Anbieterübergreifende Einwilligungsmanagementsysteme aus der Praxis

Während die bereits vorgestellten Praxisbeispiele immer vom jeweiligen Anbieter betrieben werden, gibt es Bestrebungen, Einwilligungsmanagementsysteme anzubieten, die Nutzerinnen und Nutzer befähigen, global und zentralisiert alle Einwilligungen, die von unterschiedlichen Anbietern eingefordert werden, zu verwalten. Dies ist auch eine Forderung der Datenethikkommission. In ihrem Gutachten bringt sie zum Ausdruck, dass sie ein großes Potenzial in innovativen Datenmanagement- und Datentreuhandssystemen sieht.¹⁸⁷

Es ist jedoch wichtig zu betonen, dass sich keines dieser Modelle im Massenmarkt durchgesetzt hat. Außerdem sind die Modelle zum Teil noch nicht ausgereift und stehen nicht zur Nutzung zur Verfügung.

2.2.3.1. Personal Information Management Services (PIMS) und Privacy Management Tools (PMT)

Die Idee der sog. PIMS bzw. PMT ist es, alle Daten, die von Datenverarbeitern erhoben werden, einzusehen, in einem Datenkonto zu speichern und innerhalb des Services Einwilligungen nachträglich zu entziehen oder hinzuzufügen. Die von der Stiftung Datenschutz behandelten PIMS haben sich jedoch größtenteils nicht auf dem Markt etabliert (Horn et al., 2017).¹⁸⁸

Das Unternehmen *digi.me* bietet eine (reduzierte) Variante eines PIMS/PMT an, bei dem personenbezogene Daten in einer Private Sharing App verwaltet und für einzelne Anwendungen freigegeben werden können. Als Datenquellen können bspw. Daten, die in sozialen Netzwerken gespeichert sind, genutzt werden.

¹⁸⁷ Datenethikkommission (2019). Gutachten der Datenethikkommission. Abgerufen von:

https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=D320786A39EF7EA4BCD184251FE7831A.1_cid364?_blob=publicationFile&v=6 (15.03.2020)

¹⁸⁸ Darüber hinaus sei auf das Positionspapier des Verbraucherzentrale Bundesverband (vzbv) verwiesen. vzbv (2020). Personal Information Management Systems (PIMS). Chancen, Risiken und Anforderungen. Abgerufen von: https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (09.04.2020)

Mit diesen Daten werden Anwendungen gespeist, die bspw. das Posting-Verhalten analysieren oder Gesundheitsdaten verwalten.

Abbildung 18 zeigt die Einwilligungsoberfläche für eine Anwendung zur Analyse des eigenen Social Media Verhaltens. Nach Freigabe der externen Daten, bspw. aus Konten in sozialen Medien, werden diese in der „TFP“-Anwendung analysiert und für die Nutzerinnen und Nutzer interpretiert. So können Nutzerinnen und Nutzer bspw. einsehen, ob Daten (1) dauerhaft oder kurzfristig geteilt werden, (2) sich auf dem Gerät befinden oder weitergegeben werden, (3) von anderen Nutzerinnen und Nutzern eingesehen werden können und (4) gespeichert werden. Informationen zu den Verarbeitungsarten sind dabei zugänglich und durch „Wischen“ kann eine Zustimmung erteilt werden. Da der digi.me-Kosmos sich jedoch auf eine sehr geringe Anzahl an Anwendungen insbesondere im Bereich der sozialen Medien und Gesundheitsdaten beschränkt, ist er lediglich eine kleine Variante eines PIMS / PMT.

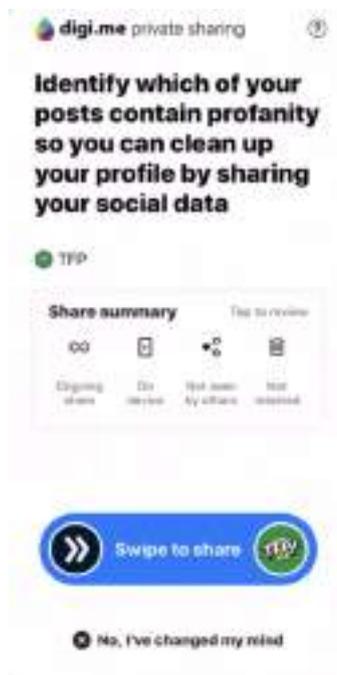


Abbildung 18: Beispiel für PIMS (digi.me)

Der Anbieter *it's my data* plant ein ähnliches Datenmanagementsystem, ist jedoch in seiner Entwicklung bisher noch nicht so weit fortgeschritten. Es ist vorgesehen, dass Nutzerinnen und Nutzer ihre Daten bei externen Anbietern wie sozialen Netzwerken oder Finanzdienstleistern abrufen und sie in einem persönlichen Datenkonto abspeichern. Eine prototypische Darstellung mit möglichen Funktionen, Voreinstellungen und Erläuterungen ist bisher nicht verfügbar, eine schematische Darstellung des *it's my data*-Systems findet sich jedoch in Abbildung 19.

Zusätzlich sollen Nutzerinnen und Nutzer ihre Daten im Konto korrigieren und löschen können und über die Datenverwaltung hinaus sind weitere Funktionen vorgesehen. Zum einen soll es ab Mitte 2020 möglich sein, Daten zu monetarisieren, zum anderen können Nutzerinnen und Nutzer bei *it's my data* ein Bonitätszertifikat anfordern.



Abbildung 19: Schematische Darstellung eines PIMS (it's my data)

2.2.3.2. Übergreifende Einwilligungsmanagementsysteme

Neben den PIMS, in denen Daten in einem zentralen Konto verwaltet werden, gibt es Anwendungen, die Einwilligungen bei externen Anbietern sichtbar machen und Einstellungen ermöglichen sollen.

Die Anwendung *Cliqz re:consent* funktioniert für eine begrenzte Anzahl von Anbietern sozialer Medien oder News-Webseiten wie für Google und Facebook. Darüber hinaus sind Anbieter des "Transparency & Consent Frameworks" des Werbewirtschaftsverbands Interactive Advertising Bureau (IAB) daran beteiligt.

Abbildung 20 zeigt die Nutzeroberfläche für die Erweiterung des Chrome-Browsers. In dieser Nutzeroberfläche können Einstellungen vorgenommen werden und Datenverarbeitungen ein- und ausgeschaltet werden. Das abgebildete Beispiel zeigt die Einstellungsmöglichkeiten für ein Facebook-Konto. Dabei wird – wie im Nutzerkonto selbst – über verschiedene Datenverarbeitungen differenziert. Möchten Nutzerinnen und Nutzer Änderungen vornehmen, können sie diese über die Erweiterung vornehmen und bspw. inaktive Datenverarbeitungen mit einem Klick aktivieren.



Abbildung 20: Beispiel für übergreifendes Einwilligungsmanagementsystem (Cliqz re:consent)

2.2.4. Mobile Umgebungen

Verbraucherinnen und Verbraucher gehen mittlerweile immer häufiger mit mobilen Endgeräten wie Smartphones oder Tablets online. Um diesen Bedürfnissen gerecht zu werden, können die meisten Modelle aus der Praxis auch in mobilen Umgebungen genutzt werden.

Die Untersuchung konnte zeigen, dass die Modelle in den mobilen Umgebungen dabei nahezu identisch zu denen in stationären Umgebungen sind. Bei der Nutzerführung existieren einige gestalterische Unterschiede, die jedoch nicht die Funktionsweise der Modelle verändern. So werden in manchen mobilen Umsetzungen Informationen über mehrere Bildschirme verteilt, so dass Texte auf eine Seite passen. Darüber hinaus werden neue Tabs durch das Einblenden von Pop-Ups ersetzt.

2.2.5. Sonstige Funktionen

Neben den Funktionen zur Einstellung der Datenschutzeinwilligung finden sich in den Praxis- und Theoriemodellen weitere Funktionen, die interessant erscheinen:

Zum einen ergänzen einige Anbieter die Datenschutxtexte mit *bildlichen Illustrationen*. Abbildung 21 und Abbildung 22 zeigen zwei Beispiele für die Verbildlichung von Datenverarbeitungen, Datenweitergabe, Tracking und Standortdaten im jeweiligen Praxiskontext. Ziel der bildlichen Illustration ist es dabei, das Verständnis der Datenschutxtexte zu erhöhen und die Interpretierbarkeit der Datenverarbeitungen zu vereinfachen.¹⁸⁹

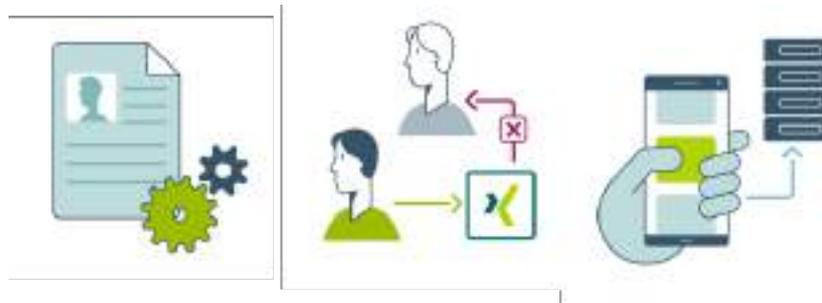


Abbildung 21: Beispiel für bildliche Untermalung von Datenschutxtexten (Datenverarbeitung, Datenweitergabe und Tracking, Xing)



Abbildung 22: Beispiel für bildliche Untermalung von Datenschutxtexten (Standortdaten, Google)

¹⁸⁹ Neben den verwendeten, individuellen Verbildlichungen, die unternehmensspezifisch gestaltet werden, gab es in der Vergangenheit Bestrebungen einheitliche Bildsymbole zu schaffen, die bei mehreren Praxispartnern integriert werden könnten. Weitere Informationen finden sich in Kettner et al. (2018).

Eine weitere Funktion, die in den Theoriemodellen identifiziert wurde, ist die *Verbildlichung von Datenströmen*. Durch diese Verbildlichung soll es Nutzerinnen und Nutzern ermöglicht werden, die Datenarten und deren Verwendung bspw. bei Drittanbietern nachzuvollziehen (vgl. Abbildung 23).

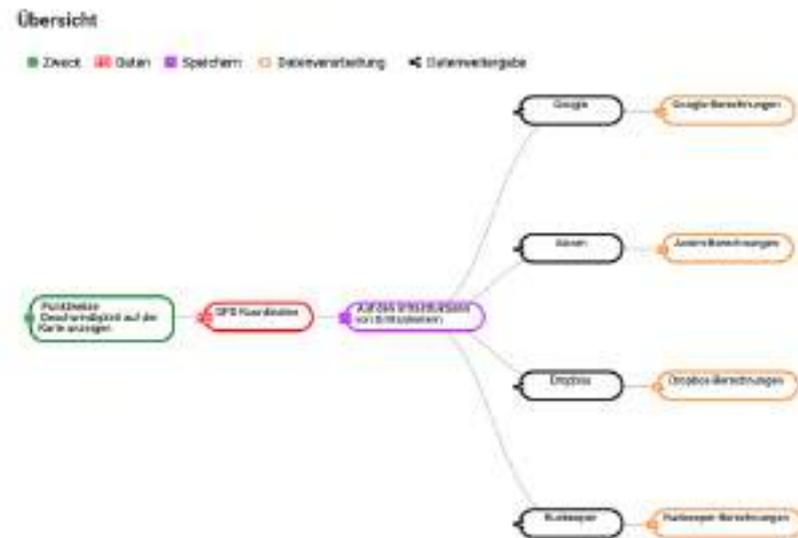


Abbildung 23: Beispiel für die Verbildlichung von Datenströmen (SPECIAL Projekt)

Eine weitere Zusatzfunktion, die bei der Untersuchung der Modelle identifiziert werden konnte, ist die *Datenschutz-Erinnerungsfunktion*. Sie wird etwa von Google angeboten und ermöglicht es den Nutzerinnen und Nutzern, eine regelmäßige Email-Erinnerung zu erhalten, die darauf hinweist, die eigenen Datenschutzeinstellungen zu überprüfen und ggf. anzupassen.

2.2.6. Zwischenfazit: Bislang gibt es nur sehr wenige differenzierte Einwilligungsmanagementsysteme in der Praxis – allerdings zeigen einige Good Practices, dass diese möglich sind

Die Darstellung der Einwilligungsmanagementmodelle aus Praxis und Theorie verdeutlicht insbesondere die folgenden Punkte: Erstens finden sich heute in der Praxis nur sehr wenige Anbieter, die ihren Kundinnen und Kunden eine differenzierte Einwilligung ermöglichen. Die bislang gängige Form sind *globale Einwilligungen*. Zweitens zeigen die wenigen Anbieter mit differenzierten Einwilligungsmanagementsystemen, dass trotz aller gegenteiliger Behauptungen eine Differenzierung grundsätzlich durchaus möglich ist. Drittens führen differenzierte Einwilligungsmanagementsysteme fast zwangsläufig dazu, dass den Verbraucherinnen und Verbrauchern auch ein *Einwilligungsmanagement im Nachhinein* ermöglicht werden muss. Auch hierfür gibt es – wenn auch nur wenige – praktische Beispiele, die aufzeigen, dass solche Cockpits umsetzbar sind. Viertens zeigt die Darstellung anbieterübergreifender Einwilligungsmanagementsysteme, dass die zugrundeliegende Idee zwar sehr naheliegend ist. Allerdings haben sich die bestehenden Ansätze (noch) nicht im Massenmarkt durchsetzen können.

2.3. Bewertung der Einwilligungsmanagementmodelle aus Praxis und Theorie

Im nächsten Schritt werden die im Abschnitt 2.2 dargestellten Einwilligungsmodelle im Hinblick auf rechtliche und verhaltenswissenschaftliche Aspekte (siehe Abschnitt 2.1) bewertet. Dabei wird auf die Vor- und Nachteile der Systeme eingegangen und überprüft, welche Verbesserungspotentiale existieren. Vor dem Hintergrund der dargestellten Umsetzungsvarianten werden die Modelle idealtypisch unterschieden und bewertet.

2.3.1. Praxisbeispiele für die Einwilligung bei Einzelanbietern

1. Globale Einwilligung durch Bestätigung

Juristische Bewertung: Eine globale Einwilligung, die Nutzerinnen und Nutzer nicht zuvor über die jeweiligen Datenverarbeitungsvorgänge informiert, hält den gesetzlichen Vorgaben für die Einwilligung nicht stand. Allerdings kann hier u. U. zur Einhaltung der rechtlichen Vorgaben ein einfach zu erreichender Link oder ein Pop-Up genügen, sofern alle erforderlichen Informationen übersichtlich und einfach erreichbar sind.

Ebenfalls unzureichend mangels Alternativen sind solche Einwilligungen, bei denen sich Nutzerinnen und Nutzer nicht ohne Einwilligung (jenseits der Vertragsdurchführung!) für den Dienst bzw. das Angebot registrieren lassen können.

Gleiches gilt für die Einwilligungen in Newsletter oder Werbeaktivitäten, ohne die Nutzerinnen und Nutzer kein Konto anlegen können bzw. den Dienst nicht nutzen können.

Verhaltenswissenschaftliche Sicht: Aus verhaltenswissenschaftlicher Sicht ist eine globale Einwilligung nicht ausreichend. Denn Verbraucherinnen und Verbraucher sind nicht in der Lage, ihre Datenschutzpräferenzen gestuft zum Ausdruck zu bringen und haben daher keine ausreichende Wahlfreiheit. Durch die aktive Bestätigung ist es sogar möglich, dass bei Verbraucherinnen und Verbrauchern eine *Kontrollillusion* entsteht, denn sie stimmen aktiv zu (Langer, 1975). Hierdurch entsteht der subjektive Eindruck, eine Wahl gehabt zu haben, obwohl dies in der Realität nicht zutrifft.

Ein weiterer aus verhaltenswissenschaftlicher Sicht relevanter Faktor, der in der Praxis oftmals eingesetzt wird, ist die Gestaltung der Entscheidungssituation. So kann durch Anpassung der Schaltflächen zur Zustimmung die Entscheidung von Verbraucherinnen und Verbrauchern beeinflusst werden. Ist die Schaltfläche zur Bestätigung auffällig gestaltet, bspw. farblich hervorgehoben oder in größerer Schriftart, ist es möglich, dass Verbraucherinnen und Verbraucher stärker zur Bestätigung tendieren, auch wenn sie die Datenverarbeitungen eigentlich nicht gut finden.

Während aus juristischer Sicht eine Verlinkung der Datenschutzinformationen genügt, um (theoretisch) sicherzustellen, dass Nutzerinnen und Nutzern bekannt ist, welche Daten zu welchen Zwecken verarbeitet werden, ist dies aus verhaltenswissenschaftlicher Perspektive nicht ausreichend – denn auch hier ist es

möglich, dass Nutzerinnen und Nutzer sich nicht aktiv um die Informationen zur Datenverarbeitung bemühen und die Begleittexte lesen.

2. Differenzierung (Wahloptionen mit datensparsamen oder ohne Voreinstellungen)

Juristische Bewertung: Eine Differenzierung ist zunächst einmal dann erforderlich, wenn Daten verarbeitet werden sollen und es hierfür keine gesetzliche Grundlage gibt. Eine Differenzierung ist sowohl in der Ausgestaltungsvariante zulässig, dass eine datensparsame Voreinstellung existiert. Wer von dieser abweichen möchte, muss aktiv werden (Opt-In). Überdies ist auch die Ausgestaltungsvariante ohne Voreinstellung nach DS-GVO möglich, da hier die Freiwilligkeit gegeben und kein Opt-out vorgesehen ist.

Unzulässig ist dagegen eine Voreinstellung, bei der Nutzerinnen und Nutzer aktiv werden müssen, um keine Einwilligung zu erteilen. Mit anderen Worten: Nutzerinnen und Nutzer müssen eindeutig einwilligen; Stillschweigen oder das Nicht-Entfernen eines bereits angekreuzten Kästchens ist nicht zulässig.

Verhaltenswissenschaftliche Bewertung: Übergeordnet ist eine Differenzierung aus verhaltenswissenschaftlicher Perspektive positiv zu bewerten, denn hierdurch wird es Verbraucherinnen und Verbrauchern ermöglicht, unterschiedliche Datenverarbeitungen gemäß ihrer Präferenzen anzupassen.

Eine Vielzahl von Studien konnte zeigen, dass Voreinstellungen einen sehr großen Einfluss auf das Verbraucherverhalten haben. So verbleiben Verbraucherinnen und Verbraucher häufig mit der Voreinstellung und passen diese nur in seltenen Fällen an – selbst dann, wenn eine Anpassung sehr einfach möglich ist.¹⁹⁰ Ist die Voreinstellung in Übereinstimmung mit der Präferenz der Verbraucherinnen und Verbraucher gesetzt, ist dies positiv zu bewerten, denn dann müssen sie keine Anpassung vornehmen und es fällt kein zusätzlicher Aufwand für sie an. Problematisch wird es dann, wenn die Voreinstellung so gesetzt ist, dass sie nicht mit den Datenschutzpräferenzen der Verbraucherinnen und Verbraucher übereinstimmen. Denn so kann es passieren, dass Verbraucherinnen und Verbraucher mit der Voreinstellung verbleiben und diese nicht anpassen, obwohl ihre Präferenzen nicht mit der Wahl übereinstimmen.

Die Gründe für das Verbleiben mit Voreinstellungen sind vielfältig. Zum einen hängt dies mit dem sog. Status Quo Bias zusammen, der besagt, dass Verbraucherinnen und Verbraucher den Status Quo übermäßig gegenüber Veränderungen bevorzugen (Kahneman et al., 1991). Diese Tendenz kann insbesondere durch die Gestaltung der Entscheidungssituation beeinflusst werden. So können die Schaltflächen zur Einstellung zum einen eindeutig und bedienungsfreundlich gestaltet und so eine Anpassung immerhin erleichtert werden. Zum anderen ist es gestalterisch möglich, dass durch Hervorhebung oder Farbwahl Voreinstellungen zusätzlich verstärkt werden und so die Tendenz der Verbraucherinnen und Verbraucher zum Verbleib bekräftigt wird.

Ein weiteres Problem mit Voreinstellungen ist, dass Verbraucherinnen und Verbraucher diese in manchen Fällen falsch interpretieren. So konnte gezeigt wer-

¹⁹⁰ Siehe Acquisti et al. (2015), Schneider et al. (2018) und Acquisti et al. (2017)

den, dass eine Voreinstellung in manchen Kontexten als Empfehlung oder implizite Botschaft verstanden und so die Tendenz zum Verbleib weiter gestärkt wird.¹⁹¹

Ebenso wie das Modell mit Voreinstellungen bietet das Modell ohne Voreinstellung eine Differenzierung der Datenverarbeitungen und ermöglicht so eine passgenaue Einstellung der Datenerhebungen. Da keine Vorauswahl getroffen wurde, entscheiden Verbraucherinnen und Verbraucher prinzipiell unvoreingenommen und beide zur Auswahl stehenden Optionen verursachen dieselben Aufwände (einen Klick). Aus Usability-Sicht wird ein zusätzlicher Schritt (Klick) in Online-Kontexten jedoch oftmals negativ bewertet, da er einen zusätzlichen Aufwand im Prozess darstellt.

Ein weiterer Aspekt, der bei dieser aktiven Wahl ebenfalls eine Rolle spielt, ist die Gestaltung und Rahmung der Optionen. Auch hier können die Entscheidungen von Nutzerinnen und Nutzern durch Anpassung des Designs manipuliert werden, bspw. durch textuelle Hervorhebungen oder Formulierungen. Die Anordnung der Optionen wurde in den untersuchten Fällen vertikal vorgenommen. Dies ist aus verhaltenswissenschaftlicher Sicht einer horizontalen Anordnung vorzuziehen, da Studien zeigen konnten, dass eine vertikale Anordnung Nutzerinnen und Nutzer weniger in ihrer Wahl beeinflusst.

3. Einwilligungsmanagement im Nachhinein

Juristische Bewertung: Das ex post Management von Einwilligungen mag zwar eine sinnvolle Einrichtung darstellen; es ändert jedoch nichts daran, dass die Einwilligung ex ante, also vor der Datenverarbeitung eindeutig und freiwillig sowie wohl informiert gegeben werden muss. Möglichkeiten, dies nachträglich zu ändern, erfüllen diese Vorgaben nicht, da sie auf ein Opt-Out hinauslaufen würden.

Verhaltenswissenschaftliche Bewertung: Ähnlich wie bei den vorherigen Modellen, bei denen Einstellungen ermöglicht werden, ist auch das Modell zum Einwilligungsmanagement im Nachhinein zunächst als positiv zu bewerten, denn Nutzerinnen und Nutzer können Datenschutzeinstellungen gemäß ihrer Präferenzen vornehmen.

Problematisch an der Herangehensweise ist jedoch, dass Nutzerinnen und Nutzer sich aktiv in das Managementsystem begeben müssen, um Einstellungen vorzunehmen. Wie bereits erwähnt, nehmen Nutzerinnen und Nutzer selten einen zusätzlichen Aufwand auf sich, um sich über Datenverarbeitungen zu informieren. Wenn bspw. Datenschutztexte hinter einem Link eingebunden werden, werden nur wenige Nutzerinnen und Nutzer diesen Link tatsächlich öffnen. Ist das Einwilligungsmanagementsystem ebenso „versteckt“ eingebunden und es bedarf eines gewissen Aufwands zur Nutzung des Systems, ist es wahrscheinlich, dass Nutzerinnen und Nutzer die Einstellungsmöglichkeiten nicht nutzen.

Grundsätzlich sind Datenschutzthemen vornehmlich vor der ersten Datenerhebung relevant und Verbraucherinnen und Verbraucher erinnern sich möglicherweise im Nachhinein nicht mehr daran, dass sie das System nutzen können.

¹⁹¹ Siehe McKenzie et al. (2006)

Diesem „Vergessen“ wird in der Praxis jedoch durch die Möglichkeit einer Erinnerungsfunktion zu Datenschutzeinstellungen entgegengewirkt. Stellen Nutzerinnen und Nutzer diese Zusatzfunktion bei der ersten Anmeldung ein, ist die Wahrscheinlichkeit prinzipiell hoch, auch im Nachhinein ein Dashboard zu nutzen.

Gestalterisch gelten ähnliche Argumente wie in den vorhergehenden Modellen. So werden Entscheidungen in Cockpits durch Gestaltung und Rahmung beeinflusst.

2.3.2. Beispiele aus der Theorie

Juristische Bewertung: Die aufgeführten Beispiele aus der Theorie erfüllen zumindest prima vista die Vorgaben der DS-GVO, indem die Nutzerinnen und Nutzer vorab die nötigen Informationen erhalten und zustimmen können, z.B. bei dem Modell der Universität Passau. Gleiches gilt für die Modelle der TU München sowie des EU-Projektes SPECIAL; hierbei wird diesseits unterstellt, dass die Nutzerinnen und Nutzer jeweils die weitere Datenverarbeitung bzw. die Einwilligung ausschließen können und die nötigen Informationen vorab erhalten. Weitere Einzelheiten ergeben sich aus den jeweiligen Projekten.

Verhaltenswissenschaftliche Bewertung: Auch bei den vorgestellten Theoriemodellen, die gemeinsam haben, eine kleinteilige und kontextspezifische Datenverwaltung zu ermöglichen, kann die Differenzierung zunächst einmal positiv bewertet werden. Die Modelle sehen für Nutzerinnen und Nutzer ausreichend Wahlfreiheit vor und ermöglichen eine individuelle Anpassung.

Während bei den Praxismodellen eine relativ grobe Differenzierung nach Datenverarbeitungen oder Zwecken vorgesehen war, ist in den Theoriemodellen eine sehr kleinteilige Differenzierung vorgesehen. So sollen Nutzerinnen und Nutzer für diverse Datenarten und diverse Unterzwecke entscheiden, welche verschiedenen Anbieter Zugriff auf die Daten haben sollen. Dieses Vorgehen bietet den Nutzerinnen und Nutzern zwar maximale Kontrolle, ist jedoch wenig praktikabel. Je mehr Datenverarbeitungen eingestellt werden können oder müssen, desto höher der Aufwand der Umsetzung. Dies ergibt sich aus der sog. „Choice Overload“-Hypothese, die besagt, dass mit einer steigenden Anzahl an Auswahloptionen nachteilige Konsequenzen einhergehen können, die dazu führen, dass Verbraucherinnen und Verbraucher weniger motiviert sind, Entscheidungen zu treffen. Im ungünstigsten Fall kann dies dazu führen, dass Verbraucherinnen und Verbraucher aufgrund der Überlastung suboptimale Auswahlen treffen (Scheibehenne et al., 2010).

Zu viel Auswahl kann außerdem zur sog. Informationsüberflutung führen, bei der es geschehen kann, dass Verbraucherinnen und Verbraucher eine Vielzahl von gleichzeitig übermittelten Informationen kognitiv nicht verarbeiten können (Eppeler & Mengis, 2004). Diese Überreizung kann ebenfalls dazu führen, dass Nutzerinnen und Nutzer den Einstellungsprozess beenden oder falsche Entscheidungen treffen. Eine verhaltenswissenschaftliche Studie konnte in diesem Zusammenhang demonstrieren, dass eine gesteigerte Auswahl dazu führen kann, dass Nutzerinnen und Nutzer mehr Daten teilen (eine größere Datenverarbeitung zulassen), wenn die Auswahl größer ist (Xu et al., 2009).

In den Theoriemodellen war darüber hinaus auffällig, dass zur Navigation der Nutzerinnen und Nutzer Hilfestellungen und Tutorials im Modell vorgesehen wurden. Zum Teil erstreckten diese sich über mehrere Seiten. Diese Hilfestellungen können Nutzerinnen und Nutzer bei der Bedienung unterstützen und die Effizienz der Nutzerführung erhöhen, jedoch sollten sie ebenfalls sparsam genutzt werden.

2.3.3. Anbieterübergreifende Einwilligungsmanagementsysteme aus der Praxis

1. PIMS / PMT

Juristische Bewertung: Die beschriebenen Datenmanagementsysteme zeichnen sich weitgehend durch die Verwaltung der bereits erhobenen Daten bzw. Einwilligungen aus. Sie mögen für die wirksame Ausübung von Widerruf oder die Transparenz bzw. die Verwaltung aller erteilten Daten von Relevanz sein; die Vorgaben der DS-GVO für den einzelnen Anbieter können diese Systeme jedoch nur dann erfüllen, wenn sie Nutzerinnen und Nutzern die nötigen Informationen *vor* der Nutzung des entsprechenden Dienstes erteilen und die Einwilligung freiwillig bleibt. Hierauf dürften die Managementsysteme allerdings kaum Einfluss haben.

Verhaltenswissenschaftliche Bewertung: Auch aus verhaltenswissenschaftlicher Sicht sind die PIMS / PMT ähnlich wie die vorhergehenden Modelle positiv zu bewerten. Nutzerinnen und Nutzer sind in der Lage, Daten aus unterschiedlichen Quellen zu kombinieren und zu entscheiden, an wen und für welche Zwecke sie Daten freigeben.

Problematisch ist jedoch, dass eine Vielzahl unterschiedlicher Datenarten und Zwecke die Komplexität erhöht und so die Praktikabilität der Nutzung leiden kann. So steigt mit der Anzahl der Einstellungsmöglichkeiten der Aufwand und es ist möglich, dass Verbraucherinnen und Verbraucher abgeschreckt werden.

Darüber hinaus spielen auch bei diesem Modell die Gestaltungsparameter eine Rolle. Je nach Wahl der Schaltflächen oder Einstellungsregler ist es für Nutzerinnen und Nutzer einfacher oder weniger einfach, die Datenverarbeitungen gemäß den eigenen Präferenzen einzustellen.

Außerdem ist es fraglich, inwieweit Verbraucherinnen und Verbraucher ein solches System tatsächlich nutzen würden, denn der Zeitpunkt der tatsächlichen Einwilligung bei den Datenverarbeitern liegt vor der Nutzung des PIMS / PMT. Wie bereits bei den Modellen zum Einwilligungsmanagement im Nachhinein ist es deshalb denkbar, dass wenige Verbraucherinnen und Verbraucher die Systeme tatsächlich nutzen.

2. Übergreifende Einwilligungsmanagementsysteme

Juristische Bewertung: Hier fällt die Beurteilung in gleicher Weise aus wie bei den PIMS / PMT: Soweit ersichtlich wirken sich übergreifende Einwilligungsmanagementsysteme nur auf bereits erteilte Einwilligungen aus, ändern also an den Voraussetzungen und der Zulässigkeit für Einwilligungen *vor* der Datenverarbeitung nichts.

Verhaltenswissenschaftliche Bewertung: Prinzipiell sind Einstellungsmöglichkeiten als etwas positives, die Wahlfreiheit förderndes, zu bewerten. Doch

auch beim Modell der übergreifenden Einwilligungsmanagementsysteme liegt der Teufel im Detail. Haben Nutzerinnen und Nutzer gegenüber bestimmten Datenverarbeitungen eine eindeutige Präferenz, d.h. „immer aktivieren“ oder „immer deaktivieren“, so können zentrale Einstellungsmöglichkeiten die Anpassungen schnell und einfach ermöglichen. Je weniger Aufwand zur Anpassung notwendig ist, desto besser.

Ist es aus Sicht der Verbraucherinnen und Verbraucher jedoch notwendig, kontextspezifisch für unterschiedliche Datenarten, Unterzwecke und Anbieter Entscheidungen zu treffen, so erhöht sich die Komplexität des Systems und der Aufwand steigt.

Weiterhin spielen, wie bei den oben genannten Modellen die Gestaltung sowie der Zeitpunkt der Einstellungsmöglichkeiten eine Rolle.

2.3.4. Weitere, übergeordnete Aspekte und Bewertung sonstiger Funktionen

Aufbereitung und Komplexität der Datenschutztexte

In allen untersuchten Praxisbeispielen wurde eine lange und technisch bzw. juristisch komplexe Datenschutzerklärung vorgefunden. In einzelnen Fällen setzten die Anbieter zur Strukturierung zwar hilfreiche Zwischenüberschriften und auch Navigationselemente wie „Drill Down“-Funktionen ein, jedoch stach keines der Beispiele besonders positiv hervor. Wie bereits in Abschnitt 2.1.2.2.1 thematisiert, ist es deshalb möglich, dass Nutzerinnen und Nutzer nicht vollständig über die Datenverarbeitungen, in die sie einwilligen, informiert sind.

Zusätzliche Hilfestellungen zu Datenverarbeitungen

Einige Praxisbeispiele sehen vor, dass Verbraucherinnen und Verbraucher bei der Nutzung des Systems eine zusätzliche über die Datenschutzerklärung hinausgehende Hilfestellung erhalten. Durch Pop-Ups oder Verlinkungen können so zusätzliche Erläuterungen zur Datenverarbeitung angeboten werden und Nutzerinnen und Nutzer erhalten ein besseres Verständnis. Diese Hilfestellungen sind grundsätzlich zu begrüßen, so lange die Erläuterungen die Informiertheit der Nutzerinnen und Nutzer fördern. Jedoch ist auch hier anzumerken, dass die Motivation der Verbraucherinnen und Verbraucher, eine solche Hilfestellung zu nutzen, begrenzt sein kann.

Bildliche Unterstützung

Sowohl Anbieter in der Praxis als auch in der Theorie sehen in ihren Modellen vor, dass Datenverarbeitungen verbildlicht werden. So existieren bereits einige Sammlungen für Privacy Icons, die einprägsam durch bildliche Sprache Datenverarbeitungsarten kommunizieren sollen (vgl. Kettner et al., 2018). Prinzipiell ist gegen eine grafische Illustration nichts einzuwenden, denn Icons können teilweise langwierige Texte ergänzen. Wenn die Icons einprägsam sind, ist es zudem möglich, schnell unterschiedliche Datenverarbeiter zu vergleichen und zu erkennen, ob Datenverarbeitungen mit den eigenen Präferenzen übereinstimmen. Problematisch ist der Einsatz von Privacy Icons jedoch dann zu bewerten, wenn durch die grafischen Abkürzungen wichtige Informationen verlorengehen. So können Privacy Icons die Datenschutztexte nicht ersetzen.

Zugänglichkeit und Sichtbarkeit der Datenschutztext-Verlinkung

In vielen der untersuchten Fälle werden Informationen zur Datenverarbeitung (Datenschutztexte) lediglich verlinkt und sind somit nur sichtbar, wenn Nutzerinnen und Nutzer diese explizit anklicken. Die Studie von Kettner et al. (2018) konnte in diesem Zusammenhang in einem Feldexperiment zeigen, dass der Anteil der Nutzerinnen und Nutzer, der einen Datenschutztext bei der Anmeldung zu einem Online-Shop tatsächlich auswählt, sehr gering ist und somit die Informiertheit der Nutzerinnen und Nutzer leidet. Im Extremfall könnte dies dafür sorgen, dass eine Einwilligung möglicherweise ohne Kenntnisnahme der Datenverarbeitung geschieht.

Die oben genannten Anbieterbeispiele zeigen, dass auch bei der Verlinkung der Datenschutzerklärung unterschiedliche Grade der Sichtbarkeit gewählt werden können. Während Beispiele existieren, die den Datenschutztext lediglich hinter dem Wort „hier“ verlinken, wählen andere Beispiele eine sichtbarere Variante und verlinken das gesamte Wort „Datenschutzerklärung“ (o. ä.). Je nachdem wie die Verlinkung also gewählt ist, können Verbraucherinnen und Verbraucher die Informationen bzw. Verlinkungen überhaupt wahrnehmen und sich letztendlich auch informieren.

Verwendung von Framing

Bei der Untersuchung der Praxisbeispiele fiel weiterhin auf, dass Datenverarbeitungen grundsätzlich sehr euphemistisch beschrieben wurden. Sprachlich wurden insbesondere Worte wie „Vertrauen“ eingesetzt und in sehr vielen Fällen wurde der Datenschutzerklärung ein Abschnitt vorangestellt, der betonte, dass dem Datenverarbeiter Datenschutz sehr wichtig sei und die Daten der Nutzerinnen und Nutzer deshalb besonders gewissenhaft verarbeitet werden. Dieses z. T. irreführende Wording wurde ausführlich vom Norwegischen Verbraucherrat (2018) untersucht und kann an plastischen Beispielen nachvollzogen werden. Aus verhaltenswissenschaftlicher Perspektive wurde die Wirkung der Rahmung bereits in Abschnitt 2.1.2.2.2 beschrieben. Grundsätzlich kann davon ausgegangen werden, dass auch in den untersuchten Praxisbeispielen eine verzerrende Wirkung auf Nutzerinnen und Nutzer hervorgerufen wird. Gerade in Fällen, in denen eine Vertrauens-Rahmung gewählt wird, ist es daher möglich, dass sich Nutzerinnen und Nutzer auf diese Aussage verlassen und deshalb keine eigenen, zusätzlichen Anstrengungen anstellen, sich unvoreingenommen über Datenpraktiken zu informieren.

Zusätzliche Hilfestellungen zur Bedienung

Einige Modelle sehen zur Unterstützung der Nutzerinnen und Nutzer bei der Bedienung der Anwendung eine zusätzliche Hilfestellung vor, die erläutert, wie Funktionen genutzt werden können. Solche Hilfestellungen können Nutzerinnen und Nutzer auch dazu befähigen, Einstellungen zur Datenverarbeitung effizienter vorzunehmen. Jedoch kann dann argumentiert werden, dass die Bedienung nicht intuitiv genug ist, wenn für sie eine Hilfestellung notwendig ist. Somit sollten Hilfestellungen sehr dosiert eingesetzt werden und können die Optimierung der intuitiven Nutzerführung nicht ersetzen.

Datenschutz-Erinnerung

Der Reizüberflutung durch die alltägliche Vielzahl relevanter, aber auch irrelevanter Informationen, begegnen Menschen mit selektiver Aufmerksamkeit, d.h. nicht benötigte Informationen werden gefiltert und ausgeblendet (Duncan, 1984;

Lavie, Hirst, De Fockert, & Viding, 2004). Dieser adaptive Mechanismus des Filterns kann allerdings auch dazu beitragen, dass eigentlich wichtige Informationen ausgefiltert und dadurch relevante Verhaltensweisen, wie beispielsweise die Anpassung von Datenverarbeitungen, vergessen werden. In einem der untersuchten Praxisbeispiele, nämlich Google, fiel eine zusätzliche Funktion besonders positiv auf, die dem Vergessen entgegenwirken kann. So können Nutzerinnen und Nutzer in ihrem Nutzerkonto einstellen, dass sie regelmäßig daran erinnert werden, ihre Datenschutzeinstellungen zu überprüfen und anzupassen. Hierdurch wird die wichtige Information regelmäßig in Erinnerung gerufen und die Selbstbestimmtheit gefördert.

Sonderfall mobile Umgebungen

Die Untersuchung der Modelle konnte zeigen, dass in der Praxis die Bedienung in einer mobilen Umgebung möglich ist. Wie in Abschnitt 2.2.4 beschrieben, wurden zwischen den stationären und mobilen Umsetzungen lediglich geringe Unterschiede festgestellt. So waren die Inhalte der mobilen Systeme meist über mehrere Seiten verteilt, um ein Scrollen zu vermeiden. Dies kann Nutzerinnen und Nutzer unterstützen und den Aufwand verringern. Jedoch muss auch hierbei bedacht werden, dass sich die Anzahl der Einstellungsmöglichkeiten auf den Aufwand auswirkt und Nutzerinnen und Nutzer bei der Bedienung frustriert werden könnten.

Ein weiteres Ergebnis der Untersuchung der mobilen Umsetzungen war, dass Informationen, die in neuen Tabs angezeigt wurden, in Pop-Ups überführt wurden. Auch diese Anpassung ist prinzipiell positiv zu bewerten, da der Aufwand der Nutzerinnen und Nutzer hierdurch verringert und die Bedienbarkeit erhöht werden. Jedoch besteht auch hier wieder die Gefahr, dass Nutzerinnen und Nutzer diese zusätzlichen Informationen nicht auswählen und so weniger informiert sind.

2.4. Vorläufige Handlungsempfehlungen

Der letzte Arbeitsschritt stellt die Verdichtung der vorhergehenden Arbeitsergebnisse dar. Ziel ist es hierbei zu definieren, welche Modelle bzw. Einzelfunktionen (Features) zum innovativen Einwilligungsmanagement grundsätzlich empfehlenswert, d.h. rechtlich zulässig und nutzerfreundlich, sind.

Aus **juristischer Sicht** sind solche Modelle zulässig, die Differenzierungen und hierbei kein Opt-Out vorsehen und die Nutzerinnen und Nutzer durch die jeweiligen Datenverarbeitungsvorgänge mit spezifischen Informationen und eindeutigen Möglichkeiten der Nicht-Einwilligung ohne Voreinstellung führen. Zudem wäre die Abgrenzung und Information der Einwilligung von den Rechtfertigungsgründen nach Art. 6 Abs. 1 b) sowie f) der DS-GVO erforderlich, um Nutzerinnen und Nutzern die Reichweite eines möglichen Widerrufs der Einwilligung zu verdeutlichen.

Aus **verhaltenswissenschaftlicher Sicht** ergibt sich der folgende, vorläufige Anforderungskatalog:

1. Ein gutes Einwilligungsmodell unterstützt grundsätzlich die **Wahlfreiheit** der Verbraucherinnen und Verbraucher und erlaubt **Einstellungsmög-**

lichkeiten, so dass Verbraucherinnen und Verbraucher Datenverarbeitungen, die sie nicht gut finden, ablehnen und solchen, die sie gut finden, zustimmen können.

2. Ein gutes Einwilligungsmodell setzt **keine oder lediglich datensparsame Voreinstellungen**.
3. Weiterhin **vermeidet** ein gutes Einwilligungsmodell eine **manipulierende Gestaltung**. Eine einfache und schnelle Möglichkeit, Einstellungen vorzunehmen sollte gewährleistet sein und Schaltflächen sollten nicht absichtlich versteckt oder betont werden.
4. **Irreführendes Framing** sowie eine **Ablenkung** vom Wesentlichen, d.h. von der Information und den Einstellungsmöglichkeiten der Datenverarbeitungen, sollten **unterlassen** werden.
5. **Visualisierungen** können Verbraucherinnen und Verbrauchern helfen, sollten jedoch **dosiert eingesetzt** werden und nicht ablenkend wirken.
6. Auch **Hilfestellungen** und zusätzliche, **unterstützende Informationen** können in einem guten Einwilligungsmodell zum Einsatz kommen, jedoch ist auch hier die **richtige Dosierung** zu beachten und Informationen sollten **freiwillig verfügbar** sein.

3. Exkurs: Cookie-Einwilligungsmodelle

Eine besondere Bedeutung haben für viele Online- bzw. E-Commerce-Anbieter sog. Cookies, die zum Sammeln von Daten während des Besuchs von (potentiellen) Kundinnen und Kunden genutzt werden, um Aufschluss über deren Verhalten und deren spezifische Interessen zu erhalten (etwa sog. Tracking-Cookies).

Zwar liegt der Fokus der vorliegenden Studie auf den Voraussetzungen und „Best Practices“ der Einwilligung in die Datenverarbeitung nach der DS-GVO, zumal hierfür entsprechende ausführliche Analysen vorliegen (Utz et al., 2019); doch werden hier aufgrund der großen Praxisrelevanz von Cookies verschiedenen Modelle kurz rechtlich sowie verhaltenswissenschaftlich beleuchtet. Dabei besteht der Anspruch der vorliegenden Studie entsprechend dem Auftrag nicht in einer erschöpfenden juristischen Bewertung; zudem konzentrieren wir uns auf die Anforderungen an die Einwilligung bei Cookies, andere Rechtfertigungstatbestände werden nicht in den Blick genommen.¹⁹²

Für die beschriebenen Cookies herrschte ein Dissens darüber, ob diese von §§ 11 ff. TMG, insbesondere § 15 TMG, oder inzwischen von der DS-GVO erfasst werden. Auf europäischer Ebene können Cookies sowohl unter die e-Privacy-Richtlinie (RL) als auch unter die DS-GVO fallen, sowohl nach Auffassung des EDSA¹⁹³ als auch schon zur Datenschutz-RL nach Auffassung des EuGH.¹⁹⁴ Nach Meinung der Datenschutzkonferenz des Bundes und der Länder (DSK)¹⁹⁵ ist aber bislang keine Umsetzung von Art. 5 Abs. 3 e-Privacy-RL in der Fassung der Richtlinie 2009/136¹⁹⁶ erfolgt.¹⁹⁷ Demgemäß würde nach Art. 95 DS-GVO diese anstatt der e-Privacy-RL eingreifen, da es an einer nationalen Umsetzung fehlt. Dementsprechend würden nach Auffassung der DSK aufgrund der Verweisung in Art. 94 Abs. 2 DS-GVO für die nötige Einwilligung die Maßstäbe der DS-GVO gelten¹⁹⁸ – und nicht diejenigen nach §§ 12, 15 TMG. Nach Auffassung der DSK ist daher eine Erklärung oder eindeutige Handlung für die Einwilligung erforderlich; dagegen reicht – entsprechend den oben dargestellten Kriterien –

¹⁹² Dazu ausführlich DSK 2019, S. 10 ff.

¹⁹³ Deutlich Europäischer Datenschutzausschuss, Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DS-GVO, insbesondere in Bezug auf die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden Ziff. 29 ff., angenommen am 12. März, abrufbar unter: 2019 https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacy-dir_gdpr_interplay_en_de.pdf

¹⁹⁴ EuGH Urt.v. 05.05.2018 - C-210/16 – Wirtschaftsakademie Rn. 33 f.

¹⁹⁵ Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Orientierungshilfe für Anbieter von Telemedien, Stand: März 2019. (DSK)

¹⁹⁶ Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABI. L 337, S. 11 ff. vom 18.12.2009.

¹⁹⁷ DSK 2019, S. 2.

¹⁹⁸ DSK 2019, S. 5.

eine bloße Untätigkeit oder bereits angekreuzte Kästchen nicht aus.¹⁹⁹ Eine Widerspruchslösung (also Opt-out) wie sie § 15 Abs. 3 TMG vorsieht, scheidet damit aus.²⁰⁰

Der BGH²⁰¹ hat nunmehr im Anschluss an die Entscheidung des EuGH²⁰² die Frage zugunsten einer europarechtskonformen Auslegung des § 15 Abs. 3 TMG entschieden und die Einholung einer Einwilligung mittels vorangeklickten Kästchens für unvereinbar sowohl mit Art. 4 Nr. 11 DS-GVO als auch der Art. 5 Abs. 3 der ePrivacy-RL erklärt. Es bedarf daher stets einer Einwilligung für Cookies.

Ferner ist nach Auffassung der DSK die vorherigen genaue Information über die jeweiligen Datenverarbeitungsvorgänge und ggf. einbezogene Dritte für die wirksame Einwilligung in Cookies erforderlich.²⁰³ Ausreichend ist demnach aber das Anklicken von Kästchen oder die Abgabe von Erklärungen bis hin zu technischen Einstellungen.²⁰⁴ Erforderlich ist aber im Gegensatz zu vielen im Web vorzufindenden Cookie-Hinweisen, dass auch die Möglichkeit der Fortsetzung des Besuchs der Webseite ohne Zustimmung zu Cookies ermöglicht wird bzw. das Setzen von Cookies abzulehnen.²⁰⁵

Schließlich verlangt die DSK erheblich größere Vorkehrungen bei Cookie-Einwilligungen als sie bislang üblich sein dürften:²⁰⁶

- So darf bei erstmaligen Aufrufen einer Webseite mitsamt der Aufforderung, dem Setzen von Cookies zuzustimmen, keine Voreinstellung zur Aktivierung getroffen werden. Ferner muss dieses HTML-Feld alle erforderlichen Informationen zu Zwecken der Datenverarbeitung einschließlich eingebundener Dritter enthalten.
- Bis zur Erteilung (oder Ablehnung) der Einwilligung müssen alle anderen Aktivitäten der Web-Seite zur Erfassung von Daten, insbesondere Java-Skripte, abgeschaltet bleiben.
- Nutzerinnen und Nutzer sollten dabei nicht direkt identifiziert werden; eine indirekte Identifizierung, die auf dem Endgerät gespeichert bleibt, ist jedoch möglich, so dass zukünftige Einwilligungen nicht erforderlich sind.
- Schließlich muss ein einfacher Widerruf der Einwilligung jederzeit möglich sein.

¹⁹⁹ DSK 2019, S. 5.

²⁰⁰ DSK 2019, S. 8.

²⁰¹ BGH Urteil vom 28. Mai 2020 - I ZR 7/16 - Cookie-Einwilligung II (Planet 49)

²⁰² EuGH, Urteil vom 1. Oktober 2019, C-673/17, PLANET49

²⁰³ DSK 2019, S. 8.

²⁰⁴ DSK 2019, S. 8. Ob allerdings die grundsätzliche Voreinstellung in einem Browser genügt, wird von der DSK nicht behandelt – und erscheint im Hinblick auf die vorab zu gebenden Informationen mehr als zweifelhaft.

²⁰⁵ DSK 2019, S. 10.

²⁰⁶ Zum Folgenden DSK 2019, S. 9.

Das Ergebnis der Diskussionen über eine ePrivacy-Verordnung, die im Kommissionsvorschlag in Art. 8 ein Verbot von Cookies neben anderen Ausnahmetatbeständen ohne Einwilligung des Betroffenen vorsieht,²⁰⁷ ist in diesem Rahmen noch nicht vorhersehbar.

3.1. Praxisbeispiele für die Cookie-Einwilligung bei Einzelanbietern

Utz et al. (2019) haben 1.000 Webseiten auf ihre Cookie-Praxis untersucht und konnten dabei unterschiedliche Modelle identifizieren. Während die Mehrzahl der Modelle Nutzerinnen und Nutzern keine Wahl beim Setzen der Cookies ließ oder lediglich eine Bestätigung für die Verarbeitung anforderte, verwendeten andere Anbieter zumindest ein binäres Einwilligungsmodell, bei dem neben der Zustimmung auch das Ablehnen der Cookies möglich war. Wenige weitere Anbieter sahen eine Differenzierung für unterschiedliche Zwecke vor. Die Modelle werden im Folgenden auf Basis der Ergebnisse von Utz et al. (2019) beschrieben und durch weitere Beispiele angereichert.

3.1.1. Keine Wahl oder globale Einwilligung

Laut Utz et al. (2019) nutzen 86% der untersuchten Webseiten ein Cookie-Banner, bei dem Nutzerinnen und Nutzer lediglich über die Erhebung der Cookies informiert werden oder diese aktiv bestätigen können. Ein Ablehnen der Cookies ist in diesem Modell nicht vorgesehen.

„Durch Nutzung dieser Website stimmen Sie der Verwendung von Cookies für Analysen, personalisierte Inhalte und Werbung zu. Weitere Informationen über Cookies finden Sie in unserer [Datenschutzerklärung](#).“ (Beispiel 4 Cookie-Banner einer Nachrichtenwebseite)

3.1.2. Binäre Wahl

Die Untersuchung von Utz et al. (2019) ergab, dass lediglich 4% der untersuchten Webseiten ein binäres Modell für die Einstellung von Cookies nutzten. Dabei konnten Nutzerinnen und Nutzer über Schaltflächen entweder „Zustimmen“ oder „Ablehnen“ (vgl. Abbildung 24).



Abbildung 24: Beispiel für binäre Einstellung von Cookies

²⁰⁷ 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 Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017, COM (2017) 10 final

3.1.3. Differenzierte Cookie-Einwilligung

In 8% der untersuchten Webseiten fanden Utz et al. (2019) differenzierte Einwilligungsmöglichkeiten. Hierbei konnten Nutzerinnen und Nutzer für unterschiedliche, nicht erforderliche Cookies einstellen, ob diese erhoben werden sollen oder nicht. Ähnlich wie bei den Praxismodellen zur Einwilligung aus Abschnitt 2.2.1.2 können bei den Cookie-Modellen unterschiedliche Voreinstellungen gewählt sein.

Abbildung 25 zeigt die Voreinstellungen eines Anbieters, bei dem alle Kategorien vorausgewählt sind und über Check-Boxen entfernt werden können.



Abbildung 25: Beispiel für Cookie-Banner bei dem alle Kategorien vorausgewählt sind (digi.me)

Abbildung 26 zeigt eine andere Ausgestaltung, bei der innerhalb der Menüführung bzw. Seitenleiste die jeweilige Cookie-Kategorien ausgewählt werden können. Im abgebildeten Beispiel sind die „funktionalen“ Cookies per Voreinstellung inaktiv.²⁰⁸ Sie können über einen Schalter aktiviert werden.

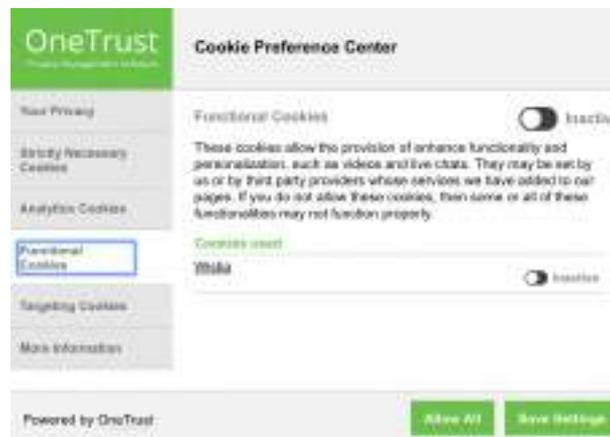


Abbildung 26: Beispiel für Cookie-Banner mit Menüführung und inaktiven Cookies (OneTrust)

Zwei weitere Ausgestaltungen, die mit vertikalen Check-Boxen und unterschiedlichen Voreinstellungen arbeiten, finden sich in Abbildung 27 und Abbildung 28.

²⁰⁸ Interessanterweise wird in diesem englischsprachigen Beispiel die Bezeichnung „funktional“ für Cookies, deren Zweck eine freiwillige Personalisierung ist, verwendet. In anderen Praxisbeispielen wird diese Begrifflichkeit zumeist für notwendige, für die Funktionen wesentliche Cookies verwendet.

Beide Anbieter stellen diese Lösungen auch gewerblich zur Verfügung und so sind diese Modelle bei diversen Unternehmen auffindbar.



Abbildung 27: Beispiel für Oberfläche zur Einstellung von Cookies mit unterschiedlichen Voreinstellungen (usercentrics)

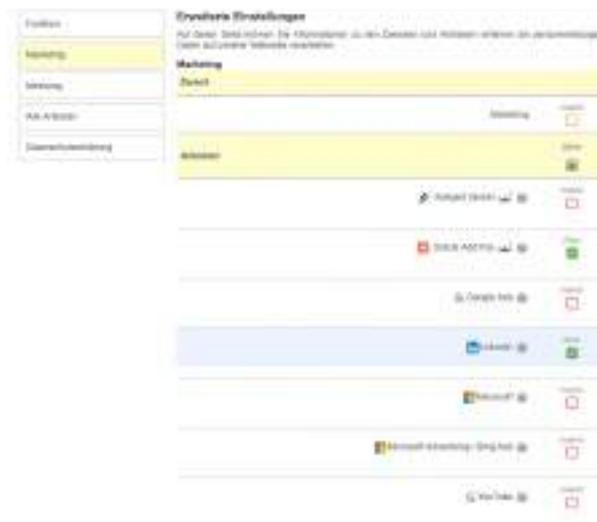


Abbildung 28: Beispiel für Oberfläche zur Einstellung von Cookies mit unterschiedlichen Voreinstellungen (consentmanager)

Eine Variante des Modells mit Wahloption ohne Voreinstellungen, in dem optionale Cookies über Check-Boxen ausgewählt werden können, findet sich in Abbildung 29. Während notwendige Cookies per Voreinstellung gesetzt sind und aufgrund ihrer Erforderlichkeit nicht entfernt werden können, sind die optionalen Cookies nicht aktiviert. Wünschen Verbraucherinnen und Verbraucher eine Aktivierung, kann dies durch zusätzliche Auswahl geschehen.



Abbildung 29: Beispiel für Cookie-Banner mit voreingestellter Datenverarbeitung („inaktiv“) und Check-Boxen (Belgian Train)

3.2. Praxisbeispiele für die globale Cookie-Einwilligung

Während die vorhergehenden Beispiele Modelle für die Einstellung von Cookies auf Einzelwebseiten umfassten, gibt es eine weitere Kategorie zum Cookie-Management. In ihr können global gesetzte Cookies über ein übergeordnetes System eingestellt werden. Eine weitere Variante zum globalen Cookie-Management wird auch über einige Browser-Plugins ermöglicht, bei denen die Cookies und Tracker auf besuchten Webseiten grundsätzlich blockiert werden, es aber über eine Nutzeroberfläche möglich ist, gewünschte Cookies wieder zu aktivieren. In den folgenden Abschnitten werden die Modelle beschrieben.

3.2.1. Differenzierter und globaler Opt-Out

Abbildung 30 zeigt die Webseite Your Online Choices, die von der European Interactive Digital Advertising Alliance (EDAA) betrieben wird. Auf der Webseite findet sich im Abschnitt „Präferenzmanagement“ eine Nutzeroberfläche, die alle Cookies und Werbetracker auflistet. Innerhalb der Liste können einzelne Cookies aktiviert oder deaktiviert werden. Außerdem bietet das System die Möglichkeit, Cookies global an- und auszuschalten.



Abbildung 30: Beispiel für globales Cookie-Management (Your Online Choices)

3.2.2. Browser Plugins

Eine weitere Möglichkeit zum übergeordneten Cookie- und Tracker-Management finden sich in Plugins für den Webbrowser Firefox. So können Nutzerinnen und Nutzer die Softwareerweiterung herunterladen und in ihrem Browser aktivieren. Alle Plugins haben gemeinsam, dass sie Cookies und Tracker per Voreinstellung blockieren. Wünschen Nutzerinnen und Nutzer jedoch, dass bestimmte Cookies erhoben werden, können diese über die Nutzeroberfläche hinzugefügt werden.

Abbildung 31 zeigt die Anwendung von Ghostery und Abbildung 32 die Anwendung von Privacy Badger.

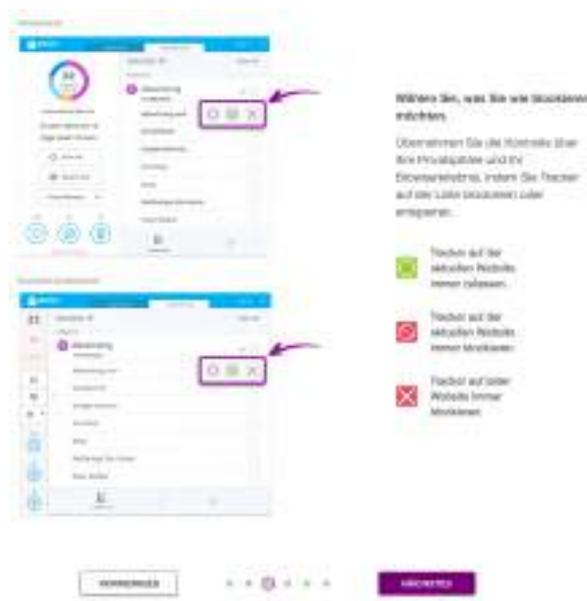


Abbildung 31: Beispiel für Browser Plugin zum Cookie-Management (Ghostery)



Abbildung 32: Beispiel für Browser Plugin zum Cookie-Management (Privacy Badger)

3.3. Bewertung der Modelle

Im nächsten Schritt werden die Cookie-Einwilligungsmodelle im Hinblick auf rechtliche und verhaltenswissenschaftliche Aspekte bewertet. Dabei wird auf die Vor- und Nachteile der Systeme eingegangen und überprüft, welche Verbesserungspotentiale existieren. Es werden **fünf Modelle** unterschieden und bewertet.

Wie bereits dargelegt, kann diese Studie auch im Hinblick auf den Gutachtenauftrag keine umfassende rechtliche Bewertung der verschiedenen Modelle leisten; insoweit sind die folgenden Ausführungen nur als grobe Einschätzungen zu verstehen, wobei die Geltung der DS-GVO unterstellt wird. Die verhaltenswissenschaftliche Bewertung kann hingegen ausführlicher vorgenommen werden, jedoch decken sich die Bewertungen für Cookies mit denen der Einwilligungsmodelle aus Abschnitt 2.3.

3.3.1. Praxisbeispiele für die Cookie-Einwilligung

1. Keine Wahl oder globale Einwilligung

Juristische Bewertung: Eine Einwilligung, bei der Nutzerinnen und Nutzer keine Möglichkeit erhalten, die Webseite auch ohne Cookie-Einwilligung zu nutzen, verstößt klar gegen das Prinzip der Freiwilligkeit. Dies gilt auch für die Modelle, die ein Opt-Out-Verfahren benutzen, da die DS-GVO derartige Verfahren nicht als freiwillig bzw. eindeutig einstuft.

Verhaltenswissenschaftliche Bewertung: Wie bereits in Abschnitt 2.3.1 beschrieben, ist eine Entscheidungssituation, in der Verbraucherinnen und Verbraucher keine Wahl haben, als negativ zu bewerten. Zwar zeichnet sich die Umsetzung durch eine hohe Praktikabilität aus, denn es müssen keine gesonderten, ggf. aufwändigen Einstellungsbemühungen unternommen werden. Wenn jedoch Nutzerinnen und Nutzer mit bestimmten Cookies nicht einverstanden sind, haben sie lediglich die Option, die Seite zu verlassen (Friss-oder-stirb-Dilemma).

Sieht das System vor, dass der Cookie-Verwendung aktiv zugestimmt werden muss, ist es sogar denkbar, dass bei den Nutzerinnen und Nutzer die sog. Kontrollillusion entsteht (Langer, 1975). Hierdurch kann bei den Nutzerinnen und Nutzern der subjektive Eindruck, eine Wahl gehabt zu haben, entstehen, obwohl dies in der Realität nicht zutrifft. Der Anbieter erscheint dadurch möglicherweise in einem besseren Licht.

2. Binäre Wahl

Juristische Bewertung: Binäre Modelle, bei denen Nutzerinnen und Nutzer die Möglichkeit erhalten, das Setzen von Cookies auszuschließen, sind uneingeschränkt zulässig – sofern keine Voreinstellung enthalten ist, dass den Cookies zugestimmt wird, und die nötigen Informationen über die Datenverarbeitung einschließlich der Weitergabe an Dritte vorab erteilt werden.

Verhaltenswissenschaftliche Bewertung: Auch aus verhaltenswissenschaftlicher Perspektive ist das binäre Modell oberflächlich zu begrüßen. So sind Zustimmung und Ablehnen einfach möglich und sehr praktikabel. Auch ist die Anzahl

der Auswahloptionen gering und Nutzerinnen und Nutzer werden nicht durch eine Vielzahl von Unteraspekten überfordert.

In der Praxis fällt jedoch häufig auf, dass die Gestaltung der Schaltflächen in Teilen manipulativ sein kann, d.h. dass Nutzerinnen und Nutzer beeinflusst werden. So werden die Schaltflächen zur Zustimmung häufig in auffälligerer Schrift gestaltet oder farblich unterlegt, so dass Nutzerinnen und Nutzer sich einer Zustimmung eher hingezogen fühlen.

3. Differenzierte Cookie-Einwilligung

Juristische Bewertung: Auch differenzierte Cookie-Einwilligungen, sofern Nutzerinnen und Nutzern auch die Möglichkeit belassen wird, überhaupt keine Cookies zu setzen, sind juristisch zulässig.

Verhaltenswissenschaftliche Bewertung: Aus verhaltenswissenschaftlicher Perspektive ist eine Differenzierung grundsätzlich ebenfalls zu begrüßen. Nutzerinnen und Nutzer können Cookies dabei gemäß ihrer Präferenzen einstellen und haben eine hohe Wahlfreiheit.

Insgesamt hängt die Praktikabilität des Modells jedoch sehr stark mit der Nutzerführung zusammen. In der Praxis werden bspw. Regler oder Check-Boxen eingesetzt, die Nutzerinnen und Nutzer aus anderen Bedienszenarien kennen und so intuitiv nutzen können. Ein weiterer Faktor, der einen Einfluss auf die Praktikabilität der Nutzung hat, ist die Granularität der Einstellungen. Zwar steigt mit der Anzahl der Optionen auch die Kontrolle der Nutzerinnen und Nutzer, jedoch ist es möglich, dass sich Nutzerinnen und Nutzer durch eine Vielzahl an Optionen überfordert fühlen und die Anpassung frustriert abbrechen.

Ein weiterer Aspekt, der bei der Differenzierung von Cookies in der Praxis eine Rolle spielt, sind die gewählten Voreinstellungen. Während manche Modelle für alle optionalen Cookies ein Opt-In vorsehen, gibt es andere Praxisbeispiele, bei denen das Setzen von Cookies voreingestellt ist. Wie bereits in Abschnitt 2.3.1 erläutert, haben Voreinstellungen eine große Wirkung auf Verbraucherinnen und Verbraucher. Wenn also die Cookie-Voreinstellungen nicht mit den Präferenzen der Nutzerinnen und Nutzer übereinstimmen, ist es möglich, dass diese dennoch mit der Voreinstellung verbleiben und so eine unerwünschte Datenverarbeitung stattfindet.

3.3.2. Praxisbeispiele für die globale Cookie-Einwilligung

1. Differenzierter und globaler Opt-Out

Juristische Bewertung: Ein globaler oder differenzierter Opt-out wäre unzulässig, ein globaler oder differenzierter Opt-in dagegen zulässig. Denn die DS-GVO verlangt stets die eindeutige Zustimmung, erlaubt aber kein erforderliches „Abwählen“ der Einwilligung. Zudem müssen die nötigen Informationen vorab erteilt werden.

Verhaltenswissenschaftliche Bewertung: Wann immer Nutzerinnen und Nutzer Webseiten (erstmalig) besuchen, erhalten sie eine webseitenspezifische, eigene Cookie-Information und müssen diese individuell einstellen. Dies kann mit der Zeit ermüdend wirken und die Aufmerksamkeit der Nutzerinnen und Nutzer reduziert sich. Dieser Ermüdung können Modelle zur globalen Einstellung von

Cookies entgegenwirken. So wird es den Nutzerinnen und Nutzern einfacher gemacht, Cookies global und übergreifend einzustellen.

Schwierig wird es aus Praktikabilitätsgründen jedoch dann, wenn die Anzahl der Einstellungsmöglichkeiten sehr hoch ist. Bei zu vielen Optionen kann sich dann die Bereitschaft der Nutzerinnen und Nutzer, Einstellungen vorzunehmen, verringern.

2. Browser Plugins

Juristische Bewertung: Für Browser-Plugins gestaltet sich die Rechtslage derzeit komplex: Denn nach Art. 5 Abs. 3 e-Privacy-RL wäre die Voreinstellung in einem Browser zulässig, nach der DS-GVO aber nicht, da die Einwilligung immer nur auf einen konkreten Datenverarbeitungsvorgang bezogen sein kann, für den jeweils ex ante die nötigen Informationen erteilt werden müssen, was bei abstrakten Voreinstellungen im Browser in der Regel nicht der Fall wäre. Da – wie hier unterstellt – die e-Privacy-RL in Art. 5 Abs. 3 aber nicht in deutsches Recht umgesetzt wurde, würde allein die DS-GVO gelten. Der BGH legt § 15 Abs. 3 TMG inzwischen europarechtskonform dahingehend aus, dass dieser den DS-GVO Vorschriften entspricht.²⁰⁹ Nur dann, wenn durch das ex ante Blockieren von Cookies über den Browser zwingend die nötigen Informationen erteilt werden, wären solche Plug-Ins zulässig; sie dürften ferner keine Einstellung zulassen, die vorab global eine Einwilligung erteilen würde. Es bedarf stets einer ausdrücklichen Einwilligung für das Setzen von Cookies.

Verhaltenswissenschaftliche Bewertung: Prinzipiell zeichnen sich die Browser Plugins durch eine hohe Wahlfreiheit aus. Die Voreinstellung, nämlich das grundsätzliche Blockieren der Cookies, kann individuell angepasst werden und Nutzerinnen und Nutzer können gewünschte Cookies aktivieren.

In den untersuchten Praxisbeispielen orientiert sich die gestalterische Umsetzung an gewohnten Nutzerführungskonzepten, bspw. mit Schaltflächen und Reglern, die einfach zu bedienen sind. Wie auch in den vorher genannten Fällen, sinkt die Praktikabilität der Einstellungsmöglichkeiten mit der Anzahl der Optionen. Je mehr Zeit Nutzerinnen und Nutzer aufwenden müssen, desto ermüdender kann der Prozess sein.

3.3.3. Weitere, übergeordnete Aspekte und Bewertung sonstiger Funktionen

Zugänglichkeit und Sichtbarkeit der Datenschutztext-Verlinkung

Auch bei den untersuchten Cookie-Modellen waren die Informationen zur konkreten Datenverarbeitung mehrheitlich hinter unauffälligen Links versteckt. Dieses Vorgehen ist, wie bereits in Abschnitt 2.3.4 beschrieben, aus informativ-sicherer Sicht als negativ zu bewerten, denn es kann davon ausgegangen werden, dass Nutzerinnen und Nutzer in den seltensten Fällen tatsächlich die verlinkten Datenschutztexte auswählen.

Framing

Auffällig bei den untersuchten Beispielen ist außerdem, dass gerade bei den Modellen ohne Einstellungsmöglichkeiten bzw. der globalen Bestätigung sehr

²⁰⁹ BGH Urt. v. 28. Mai 2020 - I ZR 7/16 - Cookie-Einwilligung II

beeinflussende Rahmungen gewählt werden. Abbildung 33 zeigt ein Beispiel für ein Cookie-Banner auf einer Webseite für Kekse (Lebensmittel), der auf dem Bestätigungsknopf eine euphorische Botschaft wählt, die Cookies (nicht Kekse) zu setzen.



Abbildung 33: Beispiel für Cookie-Banner mit positiver Rahmung (Oreo)

Ein weiteres Beispiel für den Einsatz von Framing ist das Verwenden des Wortes „Empfehlungen“ (vgl. Abbildung 34). Obwohl unklar ist, aus wessen Sicht die vorgeschlagenen Einstellungen empfehlenswert sind, kann dies einen starken Einfluss auf Nutzerinnen und Nutzer haben. Da Menschen sich gerne konform verhalten (Herdenverhalten vgl. Banerjee (1992)), ist es möglich, dass sie den Empfehlungen blind folgen, ohne darüber zu reflektieren, welche Konsequenzen das für sie hat.

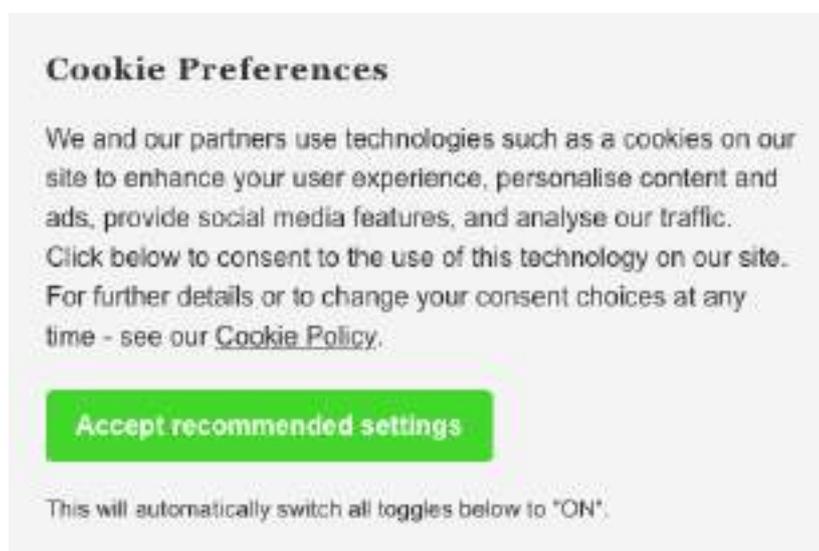


Abbildung 34: Beispiel für Cookie-Einstellungen mit Empfehlung

4. Nutzerbefragung

Wie bereits in Abschnitt 1.3.4 beschrieben, fand die Nutzerbefragung im September 2019 statt und wurde in einem Panel des Marktforschungsinstituts YouGov umgesetzt. Ziel der Befragung war es, die Erwartungen und Bedürfnisse von Verbraucherinnen und Verbrauchern an Einwilligungen und Einwilligungsmanagementsysteme zu erheben. Dabei wurden sowohl allgemeine Nutzeranforderungen und -einstellungen erhoben als auch konkrete Umsetzungen von Einwilligungsmodellen untersucht.

Im Folgenden werden die Ergebnisse der Befragung beschrieben. Im ersten Teil werden die Bewertungen von konkreten Einwilligungsmodellen aus Nutzerperspektive vorgestellt. Hiernach werden die konkreten Präferenzen von Verbraucherinnen und Verbrauchern im Hinblick auf den gewünschten Grad der Differenzierung, die Menge und Darreichungsform der Detailinformationen sowie auf Voreinstellungen vorgestellt. Im letzten Teil werden die Präferenzen der Verbraucherinnen und Verbraucher in Bezug auf Zusatzfunktionen und weitere Ergebnisse zum Datenschutzverhalten präsentiert.

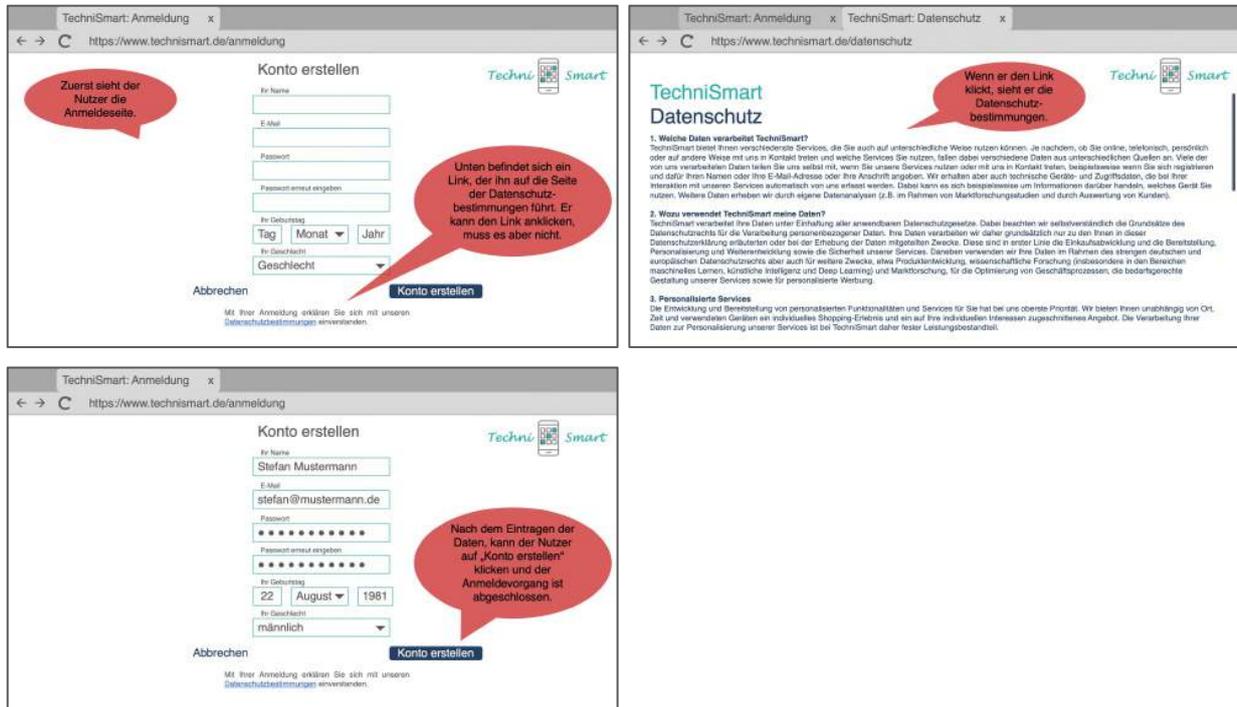
4.1. Bewertung von Einwilligungsmodellen aus Nutzerperspektive

Im ersten Teil der Befragung wurden insgesamt vier unterschiedliche Modelle getestet und von den Teilnehmerinnen und Teilnehmern im Hinblick auf sechs unterschiedliche Dimensionen bewertet.

1. Das erste Modell (v1) bildet ein *globales Einwilligungsmodell* nach, bei dem Nutzerinnen und Nutzer durch einen Text darauf hingewiesen werden, dass sie durch Anmeldung den Datenverarbeitungen gemäß Datenschutztext zustimmen. Informationen zu den Datenverarbeitungen können über einen Link zu einem neuen Tab erreicht werden. Abbildung 35 zeigt die in der Befragung verwendeten Bildschirme bzw. Screenshots.²¹⁰

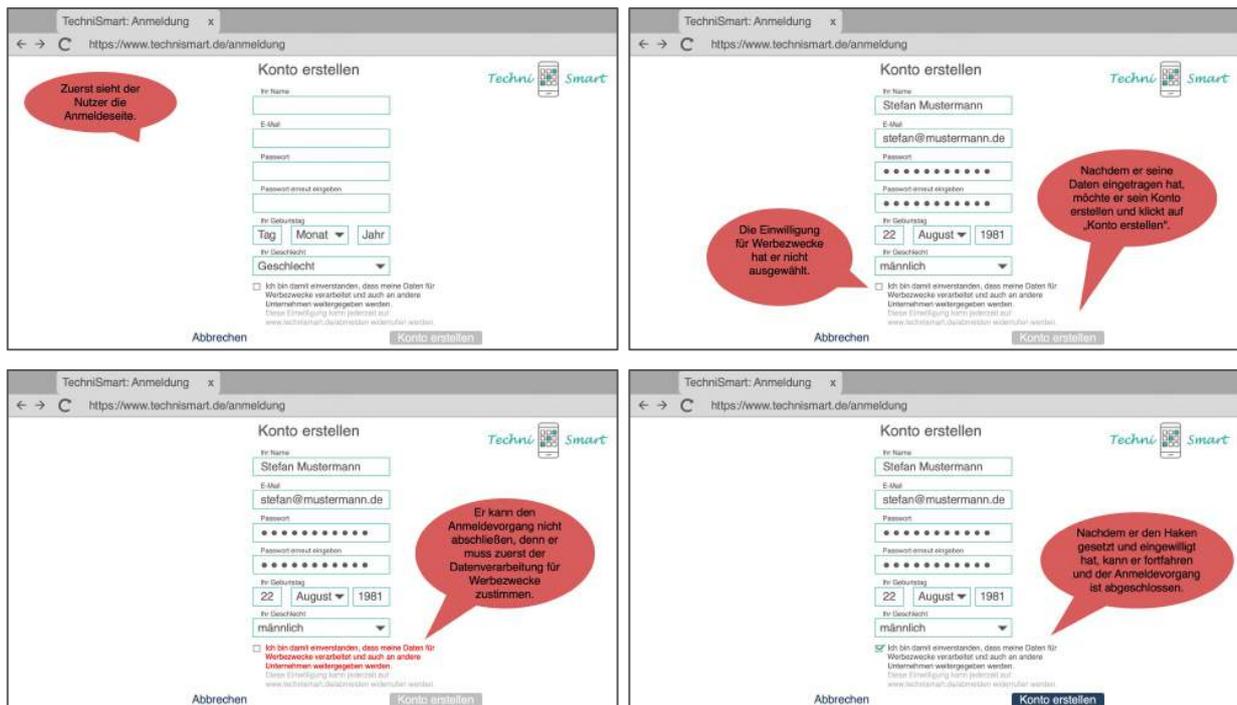
²¹⁰ Im Anhang A zum Befragungsdesign finden sich alle Screenshots der vier Modelle in einem größeren Format wieder und können dort im Detail eingesehen werden.

Abbildung 35: Befragungsdesign von Modell v1 (globale Einwilligung) auf drei Bildschirmen



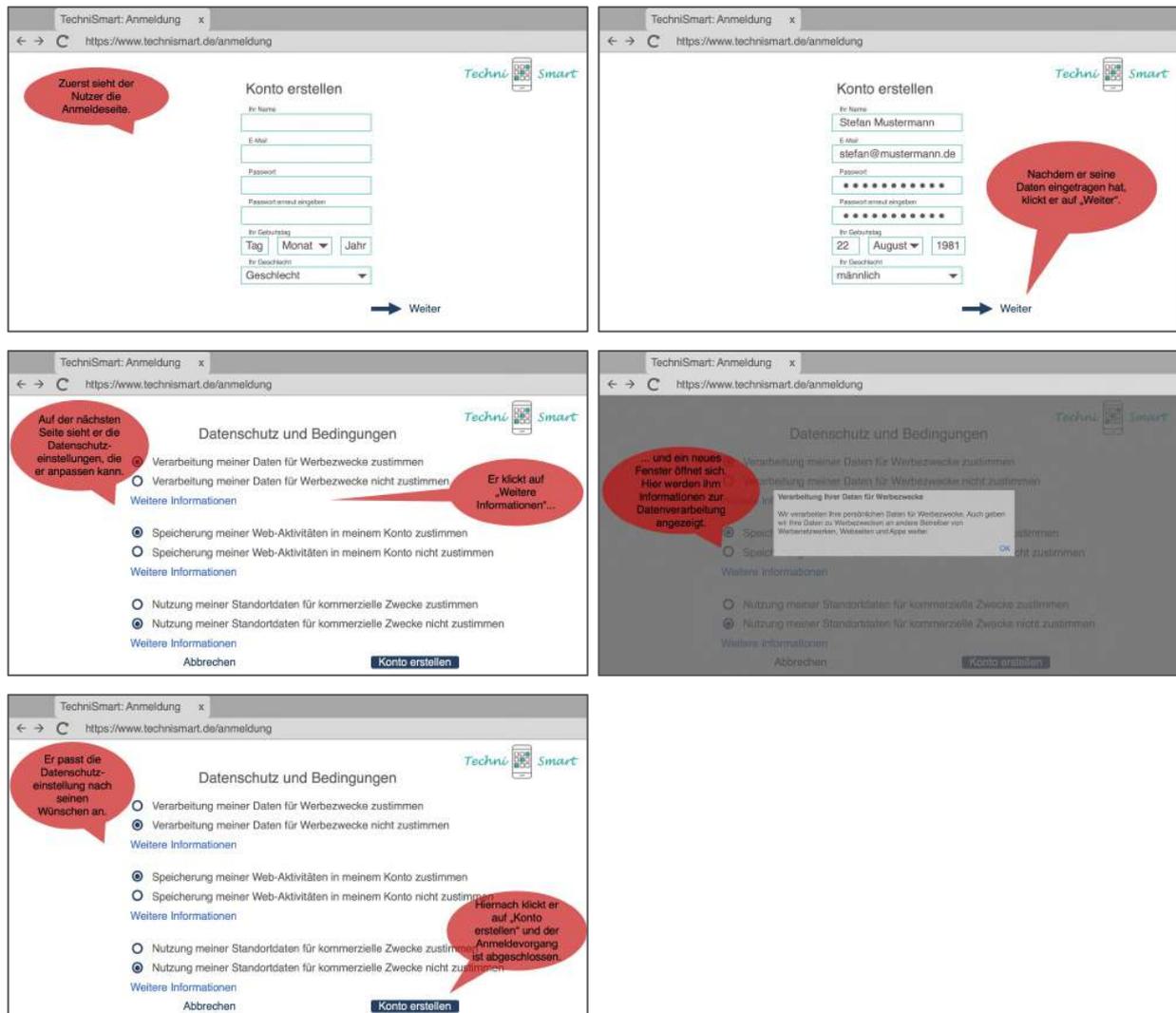
2. Das zweite Modell (v2) bildet eine *erzwungene Einwilligung* nach, bei der Nutzerinnen und Nutzer der Verarbeitung eines Datums zustimmen müssen, um fortzufahren. Eine ausführliche Erläuterung zur Verarbeitung des Datums wird nicht angeboten, jedoch wird auf die Widerrufsmöglichkeiten im Nachhinein hingewiesen. Abbildung 36 zeigt das Befragungsdesign.

Abbildung 36: Befragungsdesign von Modell v2 (erzwungene Einwilligung) auf vier Bildschirmen



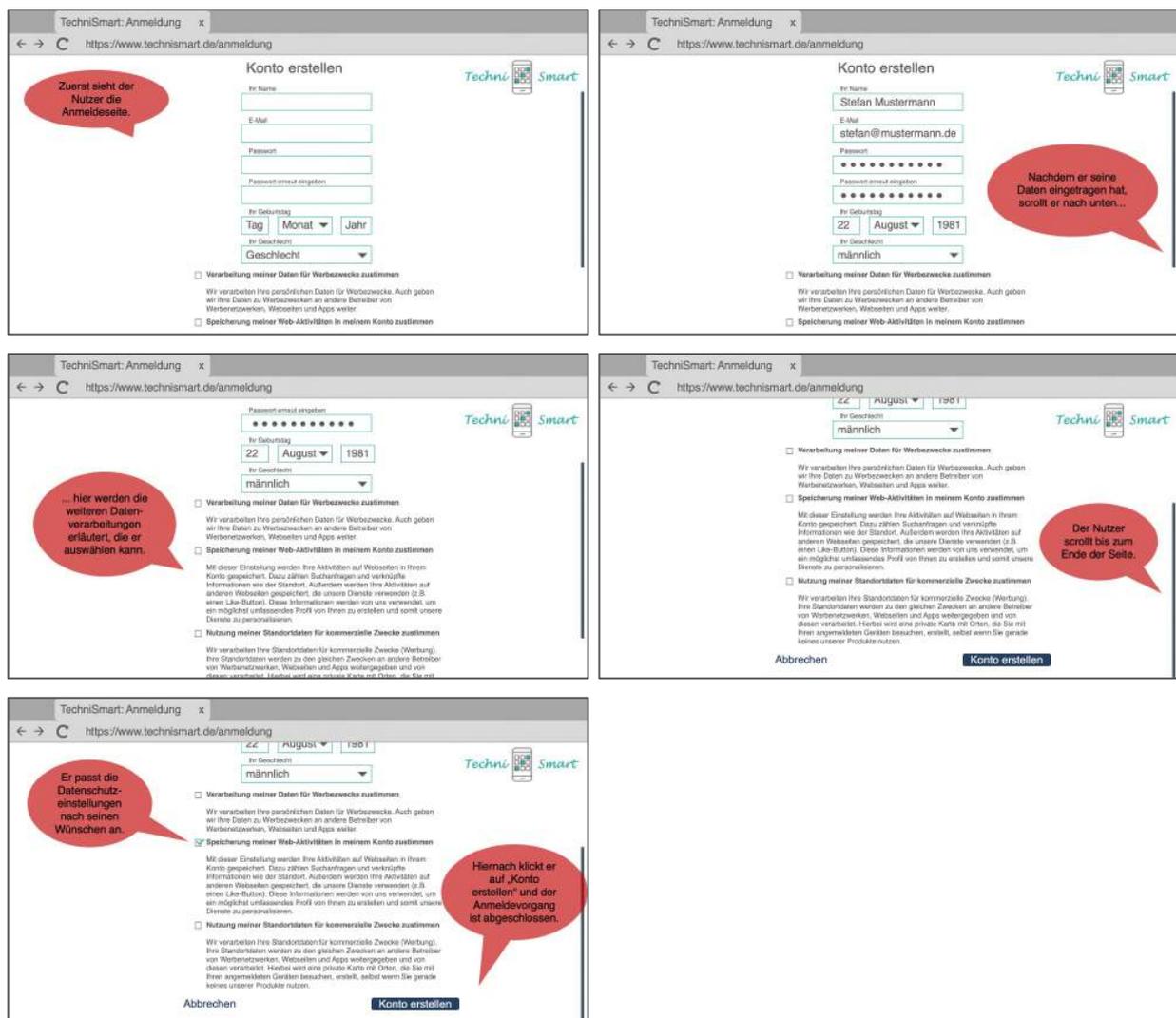
3. Das dritte Modell (v3) bildet ein *differenziertes Einwilligungsmodell* nach, bei dem drei unterschiedliche Datenverarbeitungen eingestellt werden können. Das Modell sieht dabei Voreinstellungen vor und Nutzerinnen und Nutzer können durch Anklicken der Optionen die Vorauswahl ändern. Zusätzlich sind erläuternde Informationen zu den Datenverarbeitungen über Pop-Ups erreichbar. Abbildung 37 zeigt die Screenshots, die im Befragungsdesign verwendet wurden.

Abbildung 37: Befragungsdesign von Modell v3 (differenzierte Einwilligung mit Voreinstellung und Pop-Ups) auf fünf Bildschirmen



- Das vierte Modell (v4) ist ebenfalls ein *differenziertes Einwilligungsmodell* mit drei unterschiedlichen Datenverarbeitungen. Jedoch werden die Datenverarbeitungen hierbei als *wählbare Check-Boxen* dargestellt. Die Voreinstellungen sind für alle drei Verarbeitungen nicht ausgewählt („inaktiv“), können jedoch durch einen Klick aktiviert werden. Zusätzlich werden zu den Datenverarbeitungen Erläuterungen angezeigt, die ohne zusätzlichen Aufwand im Hauptfenster einzusehen sind (vgl. Abbildung 38)

Abbildung 38: Befragungsdesign von Modell v4 (differenzierte Einwilligung mit Check-Boxen und Erläuterungen im Hauptfenster) auf fünf Bildschirmen



Alle vier Modelle leiten sich aus den Praxismodellen aus Abschnitt 2.2.1 ab und wurden den Teilnehmerinnen und Teilnehmern als Mock-Ups präsentiert. In den Modellen werden sowohl die Grade der Differenzierung, die Voreinstellungen als auch die Anzeige der Zusatzinformationen variiert.

Jeder der N=2.029 Teilnehmerinnen und Teilnehmer wurde in der Befragung zufällig zwei von vier Modellen zugeordnet. Durch die Randomisierung war es so möglich, Reihenfolgeeffekte zu minimieren. Nachdem die Teilnehmerinnen und Teilnehmer das erste zugeteilte Modell auf ihrem Bildschirm nachvollziehen

konnten, d.h. die realistische Customer Journey eines fiktiven Kunden angesehen hatten, fand die Bewertung statt.

Die Dimensionen zur Bewertung leiten sich aus der wissenschaftlichen Literatur zum HCD und der Forschung zur User Experience (UX) ab und umfassen (i) die Gesamtbewertung des Modells, (ii) die Anpassungsmöglichkeiten, (iii) das Vertrauen in den Anbieter, (iv) die Informiertheit durch die Nutzung des Modells, (v) die Einfachheit der Benutzung und (vi) die Übersichtlichkeit des Modells.

Nach der Bewertung des ersten Modells sahen die Teilnehmerinnen und Teilnehmer das zweite, zufällig ausgewählte Modell. Dieses wurde ebenfalls nach Ansicht der Customer Journey entlang der sechs Dimensionen bewertet.

Tabelle 1 zeigt die Anzahl der Observationen je Modell:

	Modell			
	v1	v2	v3	v4
Observationen	1.009	1.012	1.024	1.013

Tabelle 1: Befragungsdesign Anzahl der Observationen je Modell

4.1.1. Gesamtbewertung der Modelle

Abbildung 39 zeigt die durchschnittliche Gesamtbewertung der Customer Journey für die vier unterschiedlichen Modelle. Während Modell v2 (erzwungene Einwilligung) einen Durchschnittswert knapp über Null erhält, d.h. die durchschnittliche Bewertung ist „weder gut noch schlecht“, erzielen die anderen drei Modelle höhere durchschnittliche Bewertungen. Am höchsten ist der Mittelwert des dritten Modells (Differenzierung mit Voreinstellung und Pop-Ups).

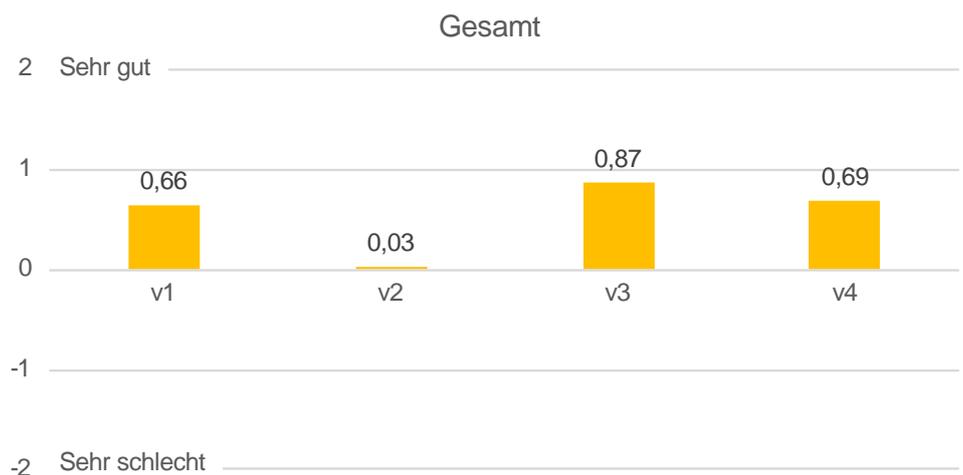


Abbildung 39: Befragungsergebnisse zur Gesamtbewertung der Einwilligungsmodelle

Hinweise: Die Fragestellung war “ Wie gut oder schlecht fanden Sie den Anmeldevorgang insgesamt?”. Die Bewertung wurde auf einer vollständig beschrifteten 5er-Skala abgefragt und die Antwortmöglichkeiten waren „Sehr gut“, „Gut“, „Weder gut noch schlecht“, „Schlecht“ und „Sehr schlecht“. Zur besseren Interpretation der Ergebnisse wurden die Antwortoptionen auf eine Skala von 2 „Sehr gut“ bis -2 „Sehr schlecht“ normiert und die Mittelwerte über alle Teilnehmerinnen und Teilnehmer berechnet. Anzahl der Observationen über alle Modelle N=2.029.

Vergleicht man die Modelle miteinander finden sich signifikante Unterschiede in den Bewertungen.^{211,212} Die Ergebnisse lassen sich wie folgt zusammenfassen:

1. *Modell v2 (erzwungene Einwilligung) schneidet im Vergleich zu den anderen Modellen insgesamt signifikant schlechter ab und die Effekte sind mittel bis groß.*
2. *Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups) schneidet insgesamt signifikant besser als die anderen Modelle ab. Im Vergleich zu den Modellen v1 (globale Einwilligung) und v4 (Differenzierung ohne Auswahl und mit Erläuterungstext) sind die Effekte jedoch lediglich klein.*

4.1.2. Anpassungsmöglichkeiten

Die Teilnehmerinnen und Teilnehmer wurden sodann gebeten zu bewerten, inwieweit die Gestaltung des jeweiligen Anmeldevorgangs es ihnen ermöglicht, ihre individuellen Bedürfnisse und Anforderungen zum Ausdruck zu bringen. Die Bewertung der Anpassungsmöglichkeiten findet sich in Abbildung 40. Die niedrigste Bewertung, d.h. geringste Zustimmung, erhält das Modell v2 (erzwungene Einwilligung), bei der die Teilnehmerinnen und Teilnehmer im Durchschnitt eher verneinen, dass eine Anpassung gemäß ihren individuellen Bedürfnissen möglich ist. Auch bei Modell v1 (globale Einwilligung) ist die Zustimmungsrate niedrig. So geben die Teilnehmerinnen und Teilnehmer an, dass die Anpassungsmöglichkeiten mittelmäßig sind.

Die beiden Differenzierungsmodelle erhalten hingegen höhere Bewertungen. Bei Modell v4 (Differenzierung ohne Auswahl und Erläuterungstext) stimmen die Teilnehmerinnen und Teilnehmer mittelmäßig bis ziemlich zu, dass Anpassungen im Anmeldevorgang möglich sind und bei Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups) ist der Zustimmungswert durchschnittlich am höchsten (ebenfalls mittelmäßige bis ziemliche Zustimmung).

²¹¹ Für alle Vergleiche wurden ungepaarte / unabhängige t-Tests (Hypothesentests) mit dem Statistikprogramm Stata berechnet. Die Unterschiede zwischen allen Modellen – bis auf den Vergleich zwischen v1 und v4 – sind signifikant auf dem 1%-Niveau.

²¹² Da die Signifikanzniveaus keine Aussage über die Größe der Unterschiede treffen, wurde zusätzlich die Effektstärke für die Vergleiche zwischen den Modellen berechnet. Die Effektstärke wurde ebenfalls mit dem Statistikprogramm Stata berechnet und für die ungepaarten / unabhängigen Variablen wurde die Maßzahl (Effektstärke) Cohens d bestimmt. Ein d zwischen 0,2 und 0,5 wurde gemäß der Konvention als kleiner Effekt, zwischen 0,5 und 0,8 als mittlerer Effekt und über 0,8 als großer Effekt interpretiert.

Zwischen Modell v2 und den anderen drei Modellen (v1, v3 und v4) lassen sich dabei *mittlere bis große Effekte* beobachten (d zwischen 0,59 und 0,8). Zwischen Modell v1 und v3 sowie v3 und v4 ist die Effektstärke immerhin klein (d=0,24 bzw. d=0,2).

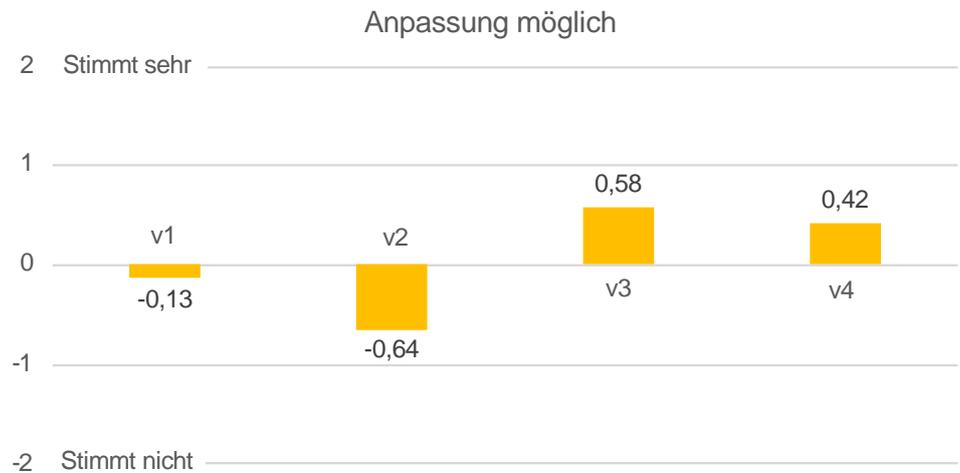


Abbildung 40: Befragungsergebnisse zur Anpassungsmöglichkeit der Einwilligungsmodelle

Hinweise: Die Fragestellung war: „Die Gestaltung des Anmeldevorgangs bietet mir die Möglichkeit der Anpassung an meine individuellen Bedürfnisse und Anforderungen“. Die Bewertung wurde auf einer vollständig beschrifteten 5er-Skala abgefragt und die Antwortmöglichkeiten waren „Stimmt sehr“, „Stimmt ziemlich“, „Stimmt mittelmäßig“, „Stimmt wenig“ und „Stimmt nicht“. Zur besseren Interpretation der Ergebnisse wurden die Antwortoptionen auf eine Skala von 2 „Stimmt sehr“ bis -2 „Stimmt nicht“ normiert und die Mittelwerte über alle Teilnehmerinnen und Teilnehmer berechnet. Anzahl der Observationen über alle Modelle N=2.029.

Die Hypothesentests zeigen, dass alle Unterschiede zwischen den Modellen signifikant sind.²¹³ Die Ergebnisse lassen sich wie folgt zusammenfassen:

1. *Modell v2 (erzwungene Einwilligung) schneidet im Vergleich zu den anderen Modellen in der Bewertung der Anpassungsmöglichkeiten signifikant schlechter ab. Insbesondere im Vergleich zu den differenzierten Einwilligungsmodellen (v3 bzw. v4) können große Effekte beobachtet werden.*
2. *Auch Modell v1 (globale Einwilligung) schneidet im Vergleich zu den Differenzierungsmodellen (v3 und v4) bei der Bewertung der Anpassungsmöglichkeiten signifikant schlechter ab, wobei mittlere Effekte gemessen werden können.*

4.1.3. Vertrauen in den Anbieter

Die Befragungsteilnehmerinnen und -teilnehmer wurden im nächsten Schritt gebeten zu bewerten, wie sehr sie einem Anbieter vertrauen, der einen solchen Anmeldevorgang zur Verfügung stellt. Die durchschnittliche Bewertung der Vertrauenswürdigkeit der Anbieter ist in Abbildung 41 zusammengefasst. Auch hier erhält Modell v2 (erzwungene Einwilligung) den schlechtesten Durchschnittswert und die Teilnehmerinnen und Teilnehmer geben an, eher abzulehnen, dass ein Anbieter mit einem solchen Anmeldevorgang vertrauenswürdig ist. Die anderen

²¹³ Allesamt auf dem 1%-Niveau.

Die Effektstärken sind – mit Ausnahme von v3 (Differenzierung mit Voreinstellung und Pop-Ups) und v4 (Differenzierung ohne Auswahl und Erläuterungstext) – durchweg mittel bis groß. Insbesondere zwischen v3 bzw. v4 und Modell v2 (erzwungene Einwilligung) können große Effektstärken gemessen werden ($d=1,08$ bzw. $d=0,94$). Zwischen v3 bzw. v4 und Modell v1 (globale Einwilligung) finden sich immerhin mittlere Effekte.

Modelle werden als eher vertrauenswürdig bewertet. Die Differenzierungsmodelle (v3 und v4) erhalten dabei etwas höhere Durchschnittswerte als das globale Einwilligungsmodell (v1).

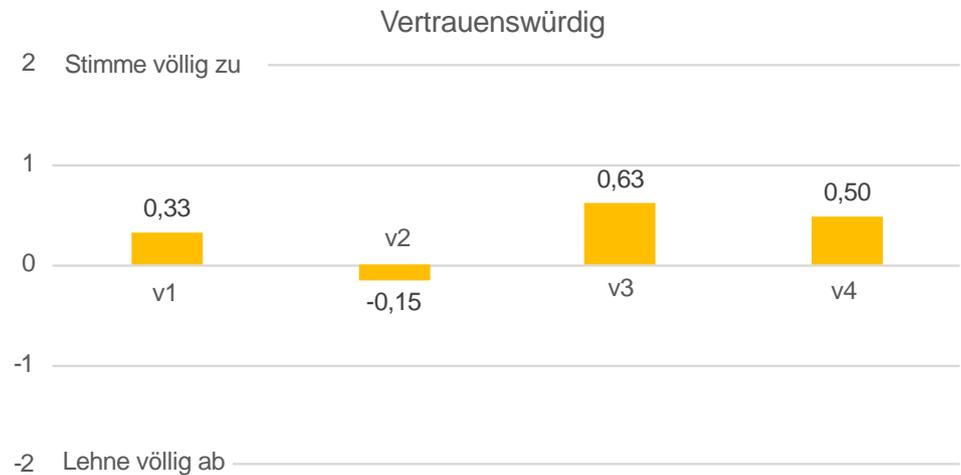


Abbildung 41: Befragungsergebnisse zur Vertrauenswürdigkeit der Einwilligungsmodelle

Hinweise: Die Fragestellung war: „Ich glaube ein Anbieter, der einen solchen Anmeldevorgang bereitstellt, ist vertrauenswürdig“. Die Bewertung wurde auf einer vollständig beschrifteten 5er-Skala abgefragt und die Antwortmöglichkeiten waren „Stimme völlig zu“, „Stimme zu“, „Weder noch“, „Lehne ab“ und „Lehne völlig ab“. Zur besseren Interpretation der Ergebnisse wurden die Antwortoptionen auf eine Skala von 2 „Stimme völlig zu“ bis -2 „Lehne völlig ab“ normiert und die Mittelwerte über alle Teilnehmerinnen und Teilnehmer berechnet. Anzahl der Observations über alle Modelle N=2.029.

Die Analyse zeigt, dass alle Unterschiede in den Mittelwerten statistisch signifikant sind.²¹⁴ Die Ergebnisse lassen sich wie folgt zusammenfassen:

1. *Modell v2 (erzwungene Einwilligung) schneidet im Vergleich zu den anderen Modellen signifikant schlechter bei der Vertrauenswürdigkeit ab. Insbesondere im Vergleich zu den differenzierten Einwilligungsmodellen (v3 bzw. v4) können große Effekte beobachtet werden.*
2. *Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups) erhält signifikant bessere Bewertungen im Hinblick auf die Vertrauenswürdigkeit als Modell v1 (globale Einwilligung). Jedoch ist der Effekt eher klein.*

4.1.4. Informiertheit

Im nächsten Schritt bewerteten die Teilnehmerinnen und Teilnehmer wie gut oder schlecht sie sich nach Abschluss des Anmeldevorgangs informiert fühlten. Hier zeigt sich ein ähnliches Bild wie auch bei den vorhergehenden Bewertungsdimensionen. Abbildung 42 fasst die Durchschnittswerte für die vier Modelle zusammen. Modell v2 (erzwungene Einwilligung) schneidet insgesamt am

²¹⁴ Allesamt auf dem 1%-Niveau.

Die Effektstärke zwischen Modell v1 (globale Einwilligung) und Modell v2 (erzwungene Einwilligung) ist immerhin klein ($d=0,49$). Für die beiden Differenzierungsmodelle v3 bzw. v4 können im Vergleich zu Modell v2 sogar große bzw. mittlere Effekte gemessen werden ($d=0,81$ bzw. $d=0,66$). Zwischen Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups) und v1 (globale Einwilligung) findet sich immerhin ein kleiner Effekt ($d=0,36$). Für die anderen Vergleiche sind die Effektstärken hingegen vernachlässigbar.

schlechtesten ab und die Teilnehmerinnen und Teilnehmer geben durchschnittlich an, eher schlecht durch das Modell informiert zu sein. Modell v1 (globale Einwilligung) erhält immerhin eine eher gute Bewertung für die Informiertheit, jedoch ist die durchschnittliche Bewertung geringer als bei den beiden Differenzierungsmodellen v3 und v4.

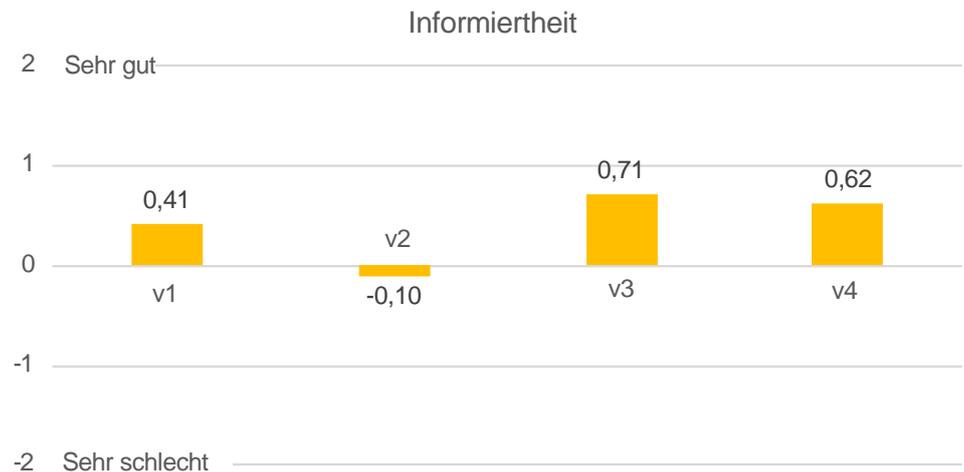


Abbildung 42: Befragungsergebnisse zur Informiertheit durch die Einwilligungsmodelle

Hinweise: Die Fragestellung war: „Wie gut oder schlecht informiert würden Sie sich nach Abschluss des Anmeldevorgangs über die Datenverarbeitungen des Anbieters fühlen?“. Die Bewertung wurde auf einer vollständig beschrifteten 5er-Skala abgefragt und die Antwortmöglichkeiten waren „Sehr gut informiert“, „Gut informiert“, „Weder gut noch schlecht informiert“, „Schlecht informiert“ und „Sehr schlecht informiert“. Zur besseren Interpretation der Ergebnisse wurden die Antwortoptionen auf eine Skala von 2 „Sehr gut informiert“ bis -2 „Sehr schlecht informiert“ normiert und die Mittelwerte über alle Teilnehmerinnen und Teilnehmer berechnet. Anzahl der Observationen über alle Modelle N=2.029.

Die Unterschiede zwischen den Mittelwerten sind signifikant²¹⁵ und die Ergebnisse lassen sich wie folgt zusammenfassen:

1. *Modell v2 (erzwungene Einwilligung) schneidet im Vergleich zu den anderen Modellen signifikant schlechter bezüglich der Informiertheit ab. Insbesondere im Vergleich zu den differenzierten Einwilligungsmodellen (v3 bzw. v4) können mittlere bis große Effekte beobachtet werden.*
2. *Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups) erhält insgesamt signifikant bessere Werte im Hinblick auf die Informiertheit. Der Unterschied ist im Vergleich zu globalen Einwilligungsmodell v1 immerhin mittel, im Vergleich zum anderen Differenzierungsmodell v4 (Differenzierung ohne Auswahl und Erläuterungstext) jedoch vernachlässigbar.*

4.1.5. Einfachheit

Darüber hinaus wurden die Teilnehmerinnen und Teilnehmer gebeten, die Einfachheit der Modelle zu bewerten. Abbildung 43 zeigt, dass für alle vier Modelle

²¹⁵ Allesamt auf dem 1%-Niveau.

Die Auswertung der Effektstärken zeigt zudem mittlere bis große Unterschiede zwischen Modell v2 (erzwungene Einwilligung) und den anderen drei Modellen. Der Effekt ist besonders groß für Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups) ($d=0,82$). Zwischen den beiden Differenzierungsmodellen v3 und v4 ist die Effektstärke vernachlässigbar und im Vergleich zum globalen Einwilligungsmodell v1 immerhin klein.

ähnliche Mittelwerte festgestellt werden können. Dies deutet darauf hin, dass die Teilnehmerinnen und Teilnehmer die Anmeldevorgänge (eher) als einfach bewerten.

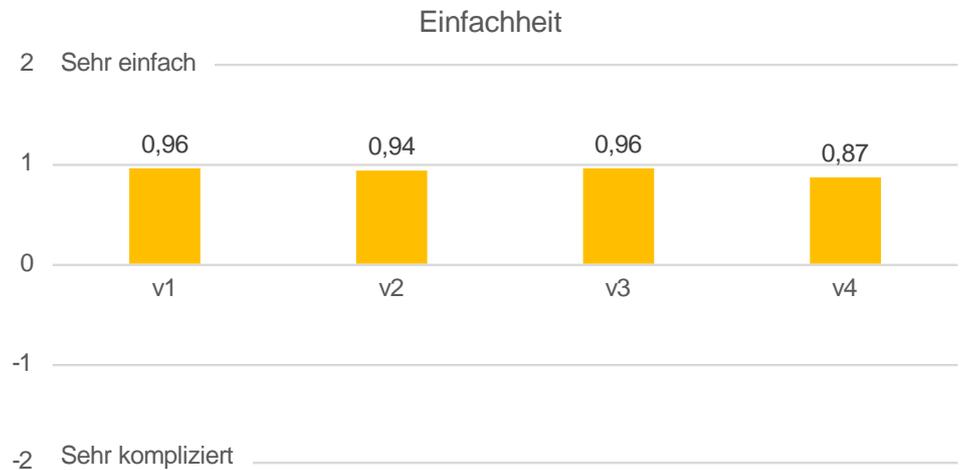


Abbildung 43: Befragungsergebnisse zur Einfachheit der Einwilligungsmodelle

Hinweise: Die Fragestellung war: „Wie einfach oder kompliziert fanden Sie den Anmeldevorgang?“. Die Bewertung wurde auf einer vollständig beschrifteten 5er-Skala abgefragt und die Antwortmöglichkeiten waren „Sehr einfach“, „Einfach“, „Weder einfach noch kompliziert“, „Kompliziert“ und „Sehr kompliziert“. Zur besseren Interpretation der Ergebnisse wurden die Antwortoptionen auf eine Skala von 2 „Sehr einfach“ bis -2 „Sehr kompliziert“ normiert und die Mittelwerte über alle Teilnehmerinnen und Teilnehmer berechnet. Anzahl der Observationen über alle Modelle N=2.029.

Die Unterschiede zwischen den Modellen sind nur vereinzelt signifikant und die Hypothesentests deuten nicht auf einen eindeutigen Effekt hin.^{216, 217} Somit lassen sich die Ergebnisse wie folgt zusammenfassen:

1. *Zwischen den Modellen kann kein systematischer Unterschied in der Bewertung der Einfachheit der Anmeldevorgänge festgestellt werden.*

4.1.6. Übersichtlichkeit

Zu guter Letzt wurden die Befragten aufgefordert, die Übersichtlichkeit der Anmeldevorgänge zu bewerten. Abbildung 44 zeigt, dass die Befragten alle Modelle als (eher) übersichtlich bewerteten, wobei Modell 3 (Differenzierung mit Voreinstellung und Pop-Ups) am besten abschneidet.

²¹⁶ Die Signifikanztests zeigen, dass lediglich zwischen Modell v1 (globale Einwilligung) und Modell v4 (Differenzierung ohne Auswahl und Erläuterungstext) sowie zwischen Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups) und Modell v4 (Differenzierung ohne Auswahl und Erläuterungstext) signifikante Unterschiede in den Mittelwerten beobachtet werden können (Signifikanzniveau 3% bzw. 2%).

²¹⁷ Darüber hinaus sind die Effektstärken bei allen Vergleichen sehr gering (maximal $d=0,1$).

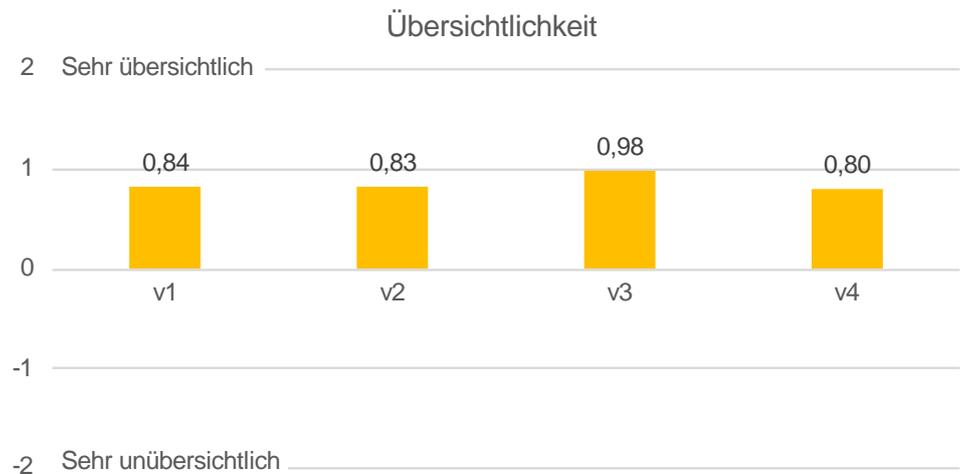


Abbildung 44: Befragungsergebnisse zur Übersichtlichkeit der Einwilligungsmodelle

Hinweise: Die Fragestellung war: „Wie übersichtlich oder unübersichtlich fanden Sie den Anmeldevorgang?“. Die Bewertung wurde auf einer vollständig beschrifteten 5er-Skala abgefragt und die Antwortmöglichkeiten waren „Sehr übersichtlich“, „Übersichtlich“, „Weder übersichtlich noch unübersichtlich“, „Unübersichtlich“ und „Sehr unübersichtlich“. Zur besseren Interpretation der Ergebnisse wurden die Antwortoptionen auf eine Skala von 2 „Sehr übersichtlich“ bis -2 „Sehr unübersichtlich“ normiert und die Mittelwerte über alle Teilnehmerinnen und Teilnehmer berechnet. Anzahl der Observationen über alle Modelle N=2.029.

Die Hypothesentest zeigen insgesamt eher kleine bis gar keine Unterschiede.²¹⁸ Die Ergebnisse lassen sich wie folgt zusammenfassen.

1. *Zwischen den vier Modellen können im Hinblick auf die Bewertung der Übersichtlichkeit keine systematischen Unterschiede festgestellt werden.*

²¹⁸ Zwar sind die Unterschiede zwischen Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups) und den anderen Modellen insgesamt signifikant (1%-Niveau), jedoch sind die Effektstärken vernachlässigbar. Zwischen den anderen Modellen können keine Unterschiede in der Bewertung festgestellt werden.

4.1.7. Zusammenfassung

Die Auswertungen der konkreten Modellbewertungen werden in Tabelle 2 nach Anteil der positiven Bewertungen innerhalb der jeweiligen Bewertungsdimensionen zusammengefasst:

Bewertungsdimension	v1	v2	v3	v4
Gesamtbewertung (Anteil sehr gut & gut)	61%	39%	70%	61%
Anpassung möglich (Anteil stimmt sehr & stimmt ziemlich)	30%	18%	56%	49%
Vertrauenswürdigkeit (Anteil stimme völlig zu & stimme zu)	42%	27%	57%	52%
Informiertheit (Anteil sehr gut informiert & gut informiert)	48%	31%	77%	58%
Einfachheit (Anteil sehr einfach & einfach)	74%	72%	75%	71%
Übersichtlichkeit (Anteil sehr übersichtlich & übersichtlich)	71%	71%	76%	69%

Tabelle 2: Zusammenfassung der Modellbewertungen nach Anteil der positiven Bewertungen über die Bewertungsdimensionen

Zwar werden bei der Bewertung der Einfachheit und Übersichtlichkeit der Modelle keine systematischen Unterschiede festgestellt, d.h. insgesamt wird die Bedienbarkeit aller Modelle eher gut bewertet, aber mit Blick auf die anderen Bewertungskategorien stellen sich klare Unterschiede heraus:

Klarer Sieger im Modellvergleich ist Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups). Es schneidet insgesamt am besten in der Gesamtbewertung ab und gerade auch in den Dimensionen Anpassungsmöglichkeiten, Vertrauenswürdigkeit und Informiertheit erhält es gute Bewertungen.

Ähnliches gilt für das zweite Differenzierungsmodell v4 (Differenzierung ohne Auswahl und Erläuterungstext), das durchweg auf dem zweiten Rang landet und im Vergleich zu den Nicht-Differenzierungsmodellen (v1 und v2) besser mit Blick auf die Dimensionen Anpassungsmöglichkeiten, Vertrauenswürdigkeit und Informiertheit abschneidet.

Modell v1 (globale Einwilligung) landet auf dem dritten Rang. Bei der Gesamtbewertung werden zwar gute Werte erzielt, jedoch finden sich Abstriche gerade mit Blick auf die Anpassungsmöglichkeiten.

Das Modell v2 (erzwungene Einwilligung) fällt bei den Verbraucherinnen und Verbrauchern durch. Nicht nur die Gesamtbewertung ist schlecht, sondern auch bei den Anpassungsmöglichkeiten, Vertrauenswürdigkeit und Informiertheit werden schlechte Bewertungen vergeben.

Tabelle 3 fasst die Rangreihenfolge der Modelle über die Bewertungsdimensionen hinweg zusammen.

Bewertungsdimension	1. Rang	2. Rang	3. Rang	4. Rang
Gesamtbewertung	v3	v4	v1	v2
Anpassung möglich	v3	v4	v1	v2
Vertrauenswürdigkeit	v3	v4	v1	v2
Informiertheit	v3	v4	v1	v2
Einfachheit	Keine systematischen Unterschiede			
Übersichtlichkeit	Keine systematischen Unterschiede			

Tabelle 3: Zusammenfassung der Modellbewertungen und Rangreihenfolge über die Bewertungsdimensionen

Darüber hinaus zeigt die Datenauswertung, dass die Ergebnisse unabhängig von Nutzertypen sind. So ist die Gesamtbewertung der Modelle bspw. unabhängig vom Alter, Geschlecht und Bildung der Befragten sowie deren Kompetenz im Bereich Datenschutz.²¹⁹

4.2. Vergleich unterschiedlicher Gestaltungsparameter

Neben den konkreten Einwilligungsmodellen, die sich an den in der Praxis identifizierten Modellen orientieren, wurden im zweiten Teil der Befragung unterschiedliche Einzelfunktionen, die in einem Einwilligungsmodell zum Einsatz kommen können, untersucht. Im ersten Schritt wurden Präferenzen mit Blick auf Voreinstellungen überprüft, im zweiten Schritt wurden unterschiedliche Differenzierungsgrade getestet und im dritten Schritt verschiedene Informationsmengen und Darreichungsformen betrachtet.

In allen drei Schritten wurden jeweils drei Ausgestaltungsoptionen paarweise miteinander verglichen. Es wurde dabei randomisiert, welche Ausgestaltungsoption links und welche rechts angezeigt wird. Hierdurch können Anzeige- bzw. Reihenfolgeeffekte minimiert werden.

Alle N=2.029 Teilnehmerinnen und Teilnehmer nahmen eine Bewertung für alle neun (3 x 3) Vergleiche vor und gaben jeweils an, welche der beiden abgebildeten Varianten sie bevorzugen würden.

4.2.1. Präferenzen zu Voreinstellungen

Die Praxisbeispiele mit Differenzierungsmöglichkeiten, die in der Bestandsaufnahme erörtert wurden (vgl. Abschnitt 2.2.1.2), sahen unterschiedliche Voreinstellungen vor. In der Befragung wurden deshalb drei Varianten, jeweils paarweise, gegeneinander getestet (vgl. Abbildung 45). Die erste Variante sieht dabei keine Voreinstellung vor und Nutzerinnen und Nutzer müssen sich bewusst entscheiden, ob sie der Datenverarbeitung zustimmen oder nicht. Die zweite Va-

²¹⁹ Die Kompetenz im Bereich Datenschutz wurde mittels mehrerer Quizfragen zum Datenschutzwissen ermittelt.

riante setzt eine Voreinstellung, dass die Daten nicht verarbeitet werden (Voreinstellung „nicht zugestimmt“), während in der dritten Variante die Datenerhebung voreingestellt ist (Voreinstellung „zugestimmt“).



Abbildung 45: Befragungsdesign "Voreinstellungen"

Abbildung 46 zeigt die Befragungsergebnisse des Vergleichs zwischen der Variante ohne Voreinstellungen und der Variante mit Voreinstellung „nicht zugestimmt“. Dabei entscheidet sich eine knappe Mehrheit von 52% für die Variante Voreinstellung „nicht zugestimmt“, während 48% die Variante ohne Voreinstellung bevorzugen.

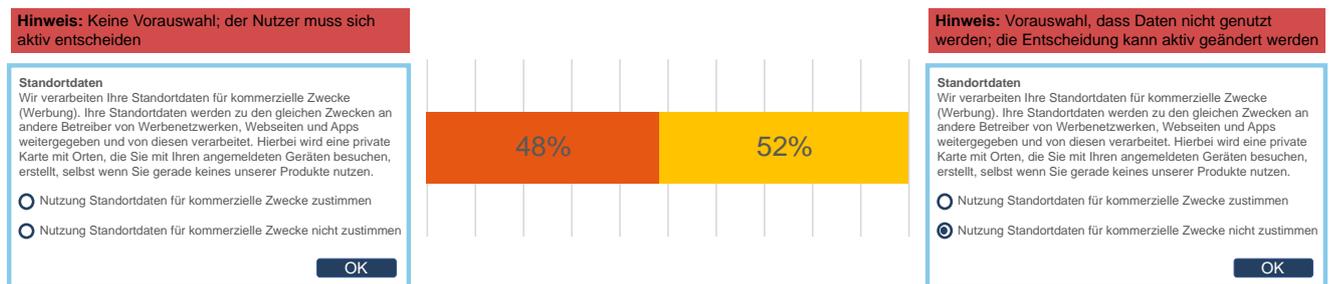


Abbildung 46: Befragungsergebnisse – keine Voreinstellung vs. Voreinstellung "nicht zugestimmt"

Hinweise: Die Aufgabenstellung war "Bitte geben Sie an, welche Version sie bevorzugen würden.". Anzahl der Observationen N=2.029.

Abbildung 47 zeigt den nächsten paarweisen Vergleich zwischen der Variante ohne Voreinstellung und der Variante mit Voreinstellung „zugestimmt“, d.h. die Datenverarbeitung ist in diesem Fall vorausgewählt. Zwei Drittel (67%) der Teilnehmerinnen und Teilnehmer bevorzugen dabei die Voreinstellung „zugestimmt“, während ein Drittel (33%) die Variante ohne Voreinstellung bevorzugt.

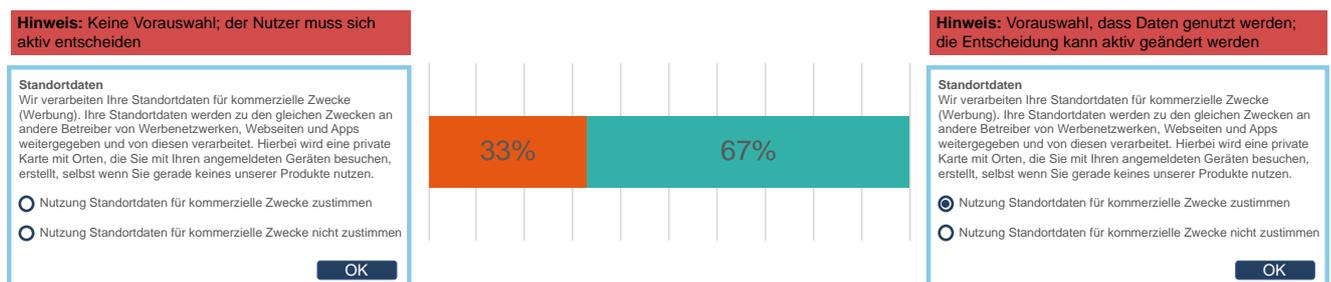


Abbildung 47: Befragungsergebnisse – keine Voreinstellung vs. Voreinstellung "zugestimmt"

Hinweise: Die Aufgabenstellung war "Bitte geben Sie an, welche Version sie bevorzugen würden.". Anzahl der Observationen N=2.029.

Im letzten Schritt werden die Ergebnisse des Vergleichs zwischen den beiden Varianten mit Voreinstellung, d.h. „nicht zugestimmt“ versus „zugestimmt“ in Abbildung 48 dargestellt. Es zeigt sich dabei ein eindeutiges Bild und so bevorzugen 71% der Befragten die Variante mit Voreinstellung „nicht zugestimmt“, d.h. keine Datenverarbeitung, während lediglich 29% die Variante mit Voreinstellung „zugestimmt“, d.h. Datenverarbeitung zugestimmt, bevorzugen.

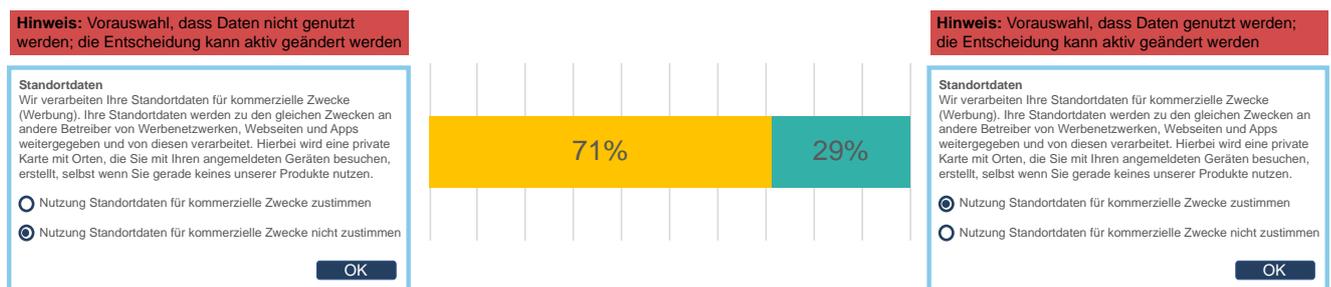


Abbildung 48: Befragungsergebnisse - Voreinstellung "nicht zugestimmt" vs. Voreinstellung "zugestimmt"

Hinweise: Die Aufgabenstellung war "Bitte geben Sie an, welche Version sie bevorzugen würden.". Anzahl der Observationen N=2.029.

Die Ergebnisse über die drei paarweisen Vergleiche hinweg lassen sich wie folgt zusammenfassen:

1. *Voreinstellungen („zugestimmt“ oder „nicht zugestimmt“) werden von den Verbraucherinnen und Verbrauchern im Vergleich zur Wahloption ohne Voreinstellung bevorzugt.*
2. *Innerhalb der Varianten mit Voreinstellungen („zugestimmt“ oder „nicht zugestimmt“) bevorzugen Verbraucherinnen und Verbraucher die Voreinstellung, in der die Daten nicht erhoben werden.*

4.2.2. Präferenzen zum gewünschten Grad der Differenzierung

Nachdem die Bestandsaufnahme zeigen konnte, dass der Grad der Differenzierung sich in der Praxis stark unterscheidet, wurden die Teilnehmerinnen und Teilnehmer zu ihren Präferenzen in Bezug auf den Differenzierungsgrad befragt. Abbildung 49 zeigt die drei getesteten Varianten. Die erste ist eine Einwilligung ohne Differenzierungsmöglichkeit (*globale Einwilligung*). Die zweite ermöglicht eine *mittlere Differenzierung* bei der zwei unterschiedlichen Verarbeitungszwecke zugestimmt werden kann. In der dritten Variante (*starke Differenzierung*) können innerhalb von zwei Verarbeitungszwecken weitere zugehörige Datenarten aktiviert bzw. deaktiviert werden. Insgesamt sind es hier fünf Verarbeitungsarten.



Abbildung 49: Befragungsdesign „Grad der Differenzierung“

Im ersten paarweisen Vergleich wurden die Präferenzen der Befragten im Hinblick auf die Varianten ohne Differenzierungsmöglichkeiten und mittlerer Differenzierung abgefragt. Die Ergebnisse finden sich in Abbildung 50. Dabei ergibt sich ein sehr eindeutiges Bild, denn 78% der Teilnehmerinnen und Teilnehmer bevorzugten die Variante mit einer mittleren Differenzierung, während lediglich 22% die Variante ohne Differenzierung bevorzugten.

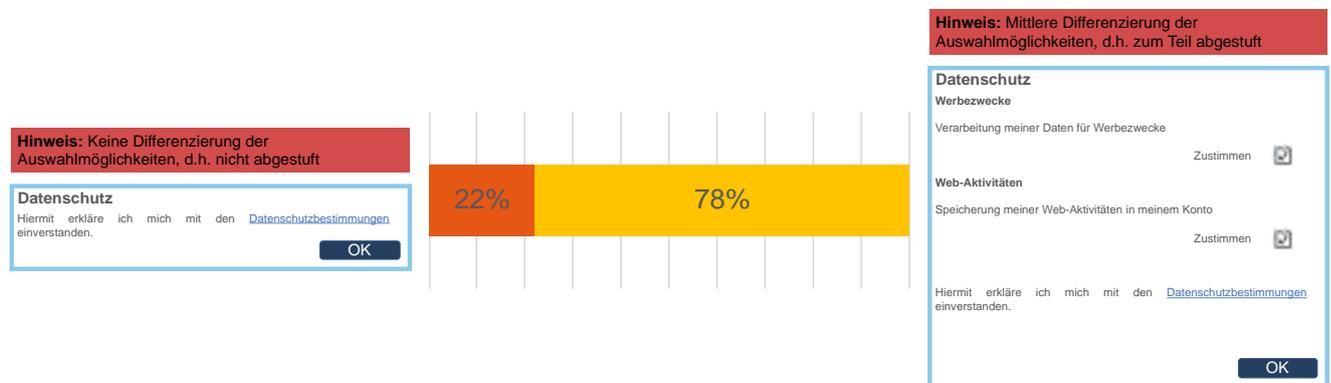


Abbildung 50: Befragungsergebnisse – keine Differenzierung vs. mittlere Differenzierung

Hinweise: Die Aufgabenstellung war "Bitte geben Sie an, welche Version sie bevorzugen würden.". Anzahl der Observationen N=2.029.

Abbildung 51 zeigt die Ergebnisse des Vergleichs zwischen der Variante ohne Differenzierung und der Variante mit starker, d.h. ausführlicher, Differenzierungsmöglichkeit. Auch hier ist die Präferenz der Teilnehmerinnen und Teilnehmer eindeutig. So bevorzugten 77% der Befragten die Variante ohne Differenzierungsmöglichkeiten und nur 23% sprechen sich für die Variante mit starker Differenzierung aus.

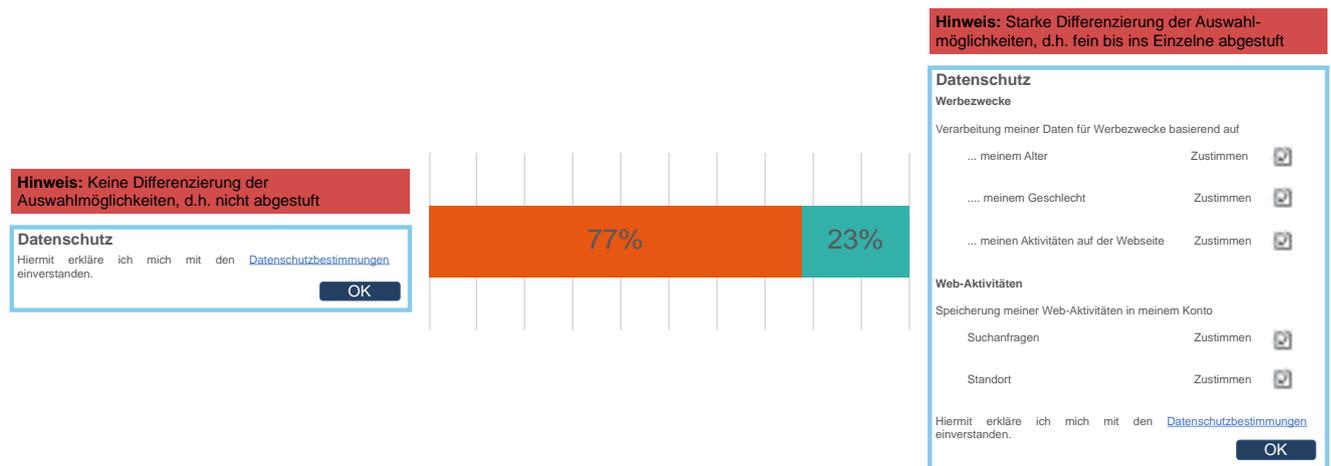


Abbildung 51: Befragungsergebnisse – keine Differenzierung vs. starke Differenzierung

Hinweise: Die Aufgabenstellung war "Bitte geben Sie an, welche Version sie bevorzugen würden.". Anzahl der Observationen N=2.029.

Im letzten Paarvergleich konnten die Teilnehmerinnen und Teilnehmer zwischen den beiden Differenzierungsvarianten entscheiden, d.h. mittlere versus starke Differenzierung. Auch hier ergibt sich ein eindeutiges Bild, welches in Abbildung 52 dargestellt ist. 69% der Befragten sprechen sich für die Variante mit starker Differenzierung aus, während 31% die Variante mit mittlerer Differenzierung wählen.

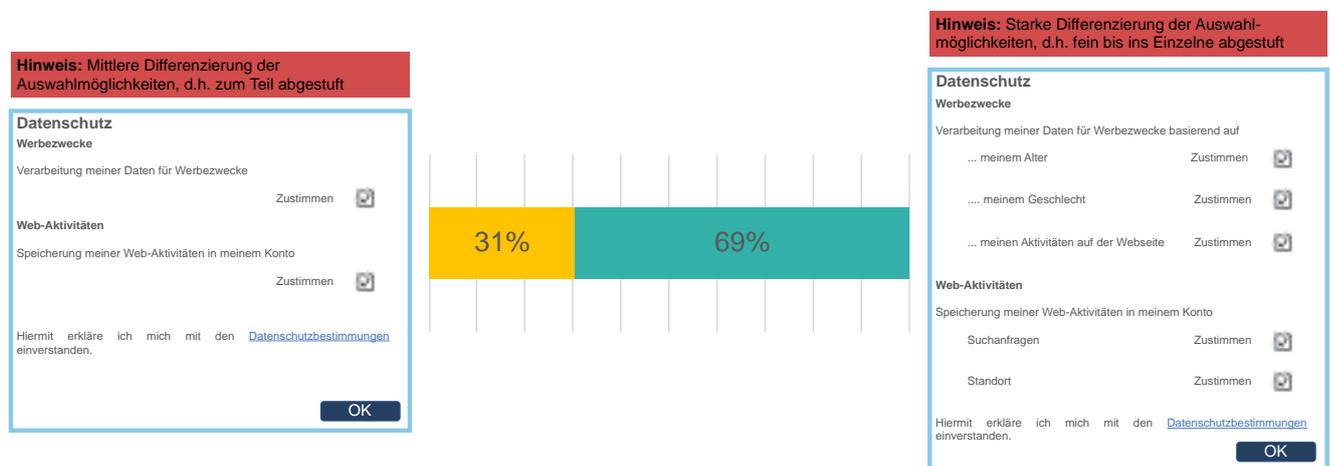


Abbildung 52: Befragungsergebnisse – mittlere Differenzierung vs. starke Differenzierung

Hinweise: Die Aufgabenstellung war "Bitte geben Sie an, welche Version sie bevorzugen würden.". Anzahl der Observationen N=2.029.

Die Ergebnisse lassen sich wie folgt zusammenfassen:

1. Verbraucherinnen und Verbraucher bevorzugen eine mittlere Differenzierung gegenüber keiner Differenzierung.
2. Verbraucherinnen und Verbraucher bevorzugen keine Differenzierung gegenüber einer starken Differenzierung.

3. Verbraucherinnen und Verbraucher bevorzugen eine starke Differenzierung gegenüber einer mittleren Differenzierung.

Betrachtet man die Ergebnisse im Ganzen, kann also festgestellt werden, dass keine eindeutige Rangreihenfolge zwischen den Varianten abgeleitet werden kann.²²⁰

4.2.3. Präferenzen zur gewünschten Menge der Informationen

Aus der Bestandsaufnahme ergibt sich, dass in den Praxisbeispielen zu Einwilligungsmodellen unterschiedliche Detailgrade zur Erläuterung der Datenverarbeitungen zu finden sind. Diese wurden für die Befragung in drei Varianten übersetzt (vgl. Abbildung 53). Die erste Variante stellt eine Einwilligungssituation dar, bei der *keine zusätzlichen Erläuterung* zur Datenverarbeitung angeboten werden. In der zweiten Variante wird eine *zusätzliche Erläuterung* zur Datenverarbeitung bereitgestellt. Die dritte Variante zeigt ebenfalls eine *zusätzliche Erläuterung* an; jedoch ist diese über ein *Pop-Up* zu erreichen.

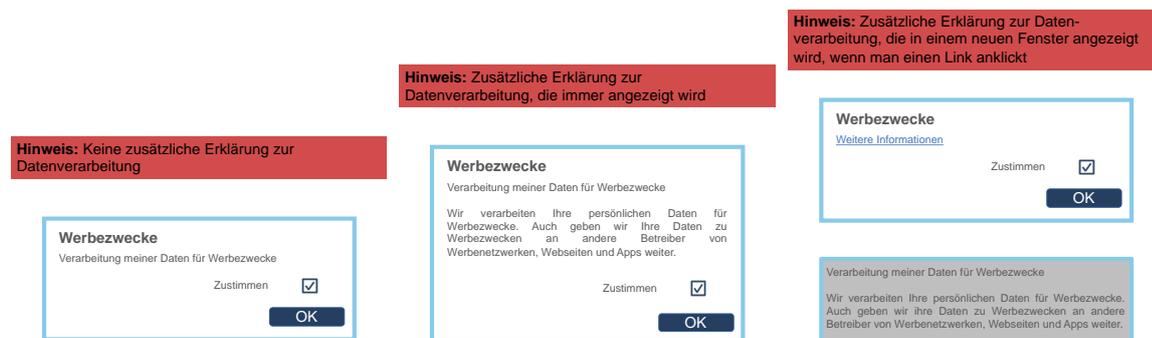


Abbildung 53: Befragungsdesign „Menge der Informationen“

Abbildung 54 zeigt die Ergebnisse des ersten paarweisen Vergleichs zwischen der Variante, die keine zusätzliche Erklärung vorsieht, und der Variante, die eine zusätzliche Erklärung vorsieht, die im Hauptfenster immer angezeigt wird. Die Ergebnisse sind dabei eindeutig und so entscheiden sich 78% der Teilnehmerinnen und Teilnehmer für die Variante mit zusätzlicher Erklärung, die immer angezeigt wird. Lediglich 22% bevorzugen die Variante ohne zusätzliche Erklärung.

²²⁰ Im Durchschnitt über alle Teilnehmerinnen und Teilnehmer entspricht das Ergebnis einer intransitiven Präferenzreihenfolge, d.h. aus Sicht der klassischen Theorie der Mikroökonomik einer „inkonsistenten“ Reihenfolge. Dies ist jedoch nicht unüblich bei der Abstimmung in Gesellschaften – auch bekannt als das Arrow-Paradox (Arrow, K. J. (1950). A difficulty in the concept of social welfare. Journal of political economy, 58(4), 328-346.)

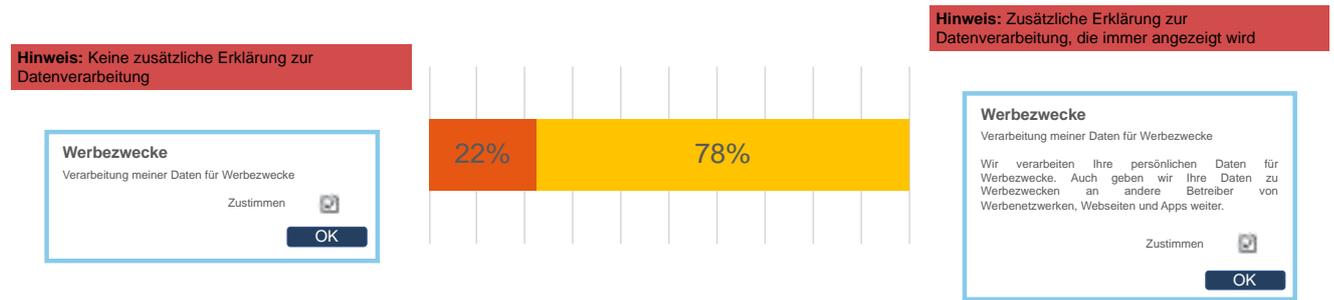


Abbildung 54: Befragungsergebnisse – keine Erklärung vs. zusätzliche Erklärung immer angezeigt

Hinweise: Die Aufgabenstellung war "Bitte geben Sie an, welche Version sie bevorzugen würden.". Anzahl der Observations N=2.029.

Auch beim nächsten paarweisen Vergleich zwischen der Variante ohne zusätzliche Erklärung und der Variante mit einer zusätzlichen Erklärung, die über ein Pop-Up geöffnet werden kann, ist das Ergebnis eindeutig (vgl. Abbildung 55). So sprechen sich 74% der Teilnehmerinnen und Teilnehmer für die Variante mit Pop-Up-Erklärung aus und lediglich 26% bevorzugen die Variante ohne eine zusätzliche Erklärung zur Datenverarbeitung.

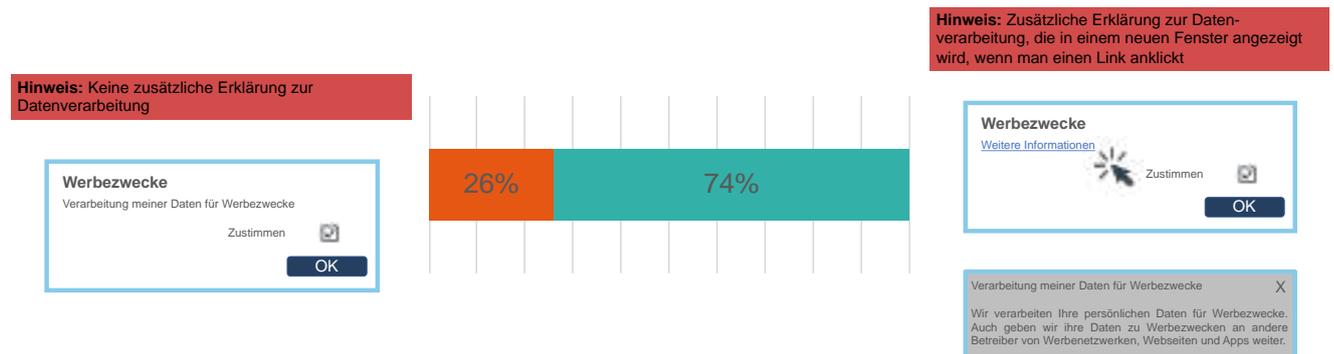
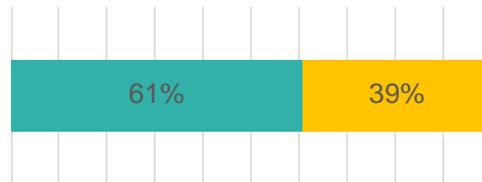


Abbildung 55: Befragungsergebnisse – keine Erklärung vs. zusätzliche Erklärung in Pop-Up

Hinweise: Die Aufgabenstellung war "Bitte geben Sie an, welche Version sie bevorzugen würden.". Anzahl der Observations N=2.029.

Im letzten Schritt entschieden die Teilnehmerinnen und Teilnehmer zwischen den beiden Varianten mit zusätzlichen Erklärungen zur Datenverarbeitung. Abbildung 56 fasst die Ergebnisse zusammen. 61% der Befragten geben an, dass sie die Variante mit Pop-Up-Erklärung bevorzugen. Die anderen 39% präferieren hingegen die Variante mit zusätzlicher Erklärung, die standardmäßig im Hauptfenster angezeigt wird.

Hinweis: Zusätzliche Erklärung zur Datenverarbeitung, die in einem neuen Fenster angezeigt wird, wenn man einen Link anklickt



Hinweis: Zusätzliche Erklärung zur Datenverarbeitung, die immer angezeigt wird



Abbildung 56: Befragungsergebnisse – zusätzliche Erklärung in Pop-Up vs. zusätzliche Erklärung immer angezeigt

Hinweise: Die Aufgabenstellung war "Bitte geben Sie an, welche Version sie bevorzugen würden.". Anzahl der Observationen N=2.029.

Insgesamt ergibt sich ein konsistentes und eindeutiges Bild für die Präferenz der Teilnehmerinnen und Teilnehmer im Hinblick auf zusätzliche Erläuterungen zu Datenverarbeitungen:

1. *Verbraucherinnen und Verbraucher bevorzugen Varianten mit zusätzlichen Erläuterungen gegenüber solchen, bei denen keine Erläuterungen angeboten werden.*
2. *Innerhalb der Varianten mit zusätzlichen Erläuterungen bevorzugen Verbraucherinnen und Verbraucher die Variante mit Pop-Up gegenüber der Variante, bei der der Erläuterungstext immer angezeigt wird.*

4.2.4. Zusammenfassung

Die Präferenzen der Verbraucherinnen und Verbraucher im Hinblick auf die Gestaltungsvarianten und Einzelfunktionen, die bei einer Einwilligung zum Einsatz kommen können, lassen sich wie folgt zusammenfassen:

Bezüglich der Bewertung von Voreinstellungen ist die Präferenzstruktur der Verbraucherinnen und Verbraucher eindeutig. So werden Voreinstellungen bevorzugt und innerhalb der Voreinstellungen die Variante, bei der die Datenverarbeitung (zunächst) als inaktiv voreingestellt ist.

Mit Blick auf den Differenzierungsgrad der Einwilligung sind die Präferenzen nicht eindeutig. Während im ersten Teil der Befragung, d.h. bei der Bewertung der vier konkreten Einwilligungsmodelle, eindeutig festgestellt werden konnte, dass Differenzierungsmodelle besser abschneiden, ist auf Grundlage der vorliegenden Detailergebnisse nicht klar, wie weit die Differenzierung reichen sollte. So sollte die Möglichkeit, Datenarten über unterschiedliche Zwecke und Verarbeiter abzufragen, nicht bis ins Unendliche übertrieben werden.

Bezüglich der Informationsmenge ist die Präferenzstruktur der Verbraucherinnen und Verbraucher klar. Zusätzliche Informationen werden insgesamt bevorzugt und am beliebtesten ist die Variante mit Pop-Ups, d.h. Verbraucherinnen und Verbraucher können die Informationen durch Öffnen eines separaten Fensters schnell und einfach erhalten. Dieses Ergebnis stimmt ebenfalls mit den Ergebnissen der Bewertung der Gesamtmodelle aus dem ersten Teil zusammen.

So wurde das Differenzierungsmodell, das Pop-Ups vorsah, insgesamt am besten beurteilt.

Insgesamt zeigen die Ergebnisse auch interessante Zusammenhänge mit Blick auf Nutzertypen. So finden sich zwar keine Effekte mit Blick auf das Alter der Befragten, d.h. die Präferenzen sind unabhängig vom Alter, jedoch zeigt sich ein Zusammenhang mit den Datenschutzkompetenzen der Befragten. Insbesondere die Präferenzen der Teilnehmerinnen und Teilnehmer mit Blick auf Voreinstellungen hängen mit dem Datenschutzwissen der Befragten zusammen. So bevorzugen insbesondere Teilnehmerinnen und Teilnehmer mit hohem Datenschutzwissen die Voreinstellungen „inaktiv“ gegenüber der Voreinstellung „aktiv“. Die Internet-Nutzungsintensität spielt hingegen keine Rolle.

4.3. Präferenzen zu Zusatzfunktionen

Neben den konkreten Ausgestaltungen der Einwilligungsmodelle wurden die Teilnehmerinnen und Teilnehmer der Befragung gebeten, unterschiedliche Zusatzfunktionen zu bewerten. So wurden bspw. das Einwilligungsmanagement im Nachhinein (Dashboards bzw. Portale) und übergeordnete Modelle, wie sie in der Theorie vorgesehen werden, bewertet. Weiterhin wurden die Möglichkeiten einer Datenschutzerinnerungsfunktion und Gestaltungsmaßnahmen wie Piktogramme oder Datenschutztexte auf einer Seite (One-Pager) bewertet.²²¹

Abbildung 57 zeigt die durchschnittlichen Bewertungen der Zusatzfunktionen. Ein Dashboard bzw. Portal zur Verwaltung und Anpassung der Daten im Nachhinein wird dabei von den Teilnehmerinnen und Teilnehmern am besten bewertet.²²² Auf dem zweiten Rang landet die Funktion, die innerhalb eines Dashboards bzw. Portals zum Einsatz kommen kann, nämlich, dass globale Einstellungsmöglichkeiten vorgenommen werden können. Der One-Pager und Piktogramme werden von den Teilnehmerinnen und Teilnehmern als eher gut bewertet. Auf den hinteren Rängen, jedoch immer noch mit einer eher guten Bewertung, finden sich die Datenschutzerinnerungsfunktion und ein übergeordnetes Datenschutzportal, in dem man Einstellungen für mehrere Dienste vornehmen kann.

²²¹ Die vollständigen Fragestellungen finden sich im Anhang A.

²²² Die Unterschiede in den Bewertungen sind dabei im Vergleich zu den anderen Funktionen signifikant (1%-Niveau) und die Effektstärken im Vergleich zur Erinnerungsfunktion und dem übergeordneten Datenschutzportal klein bis mittel.

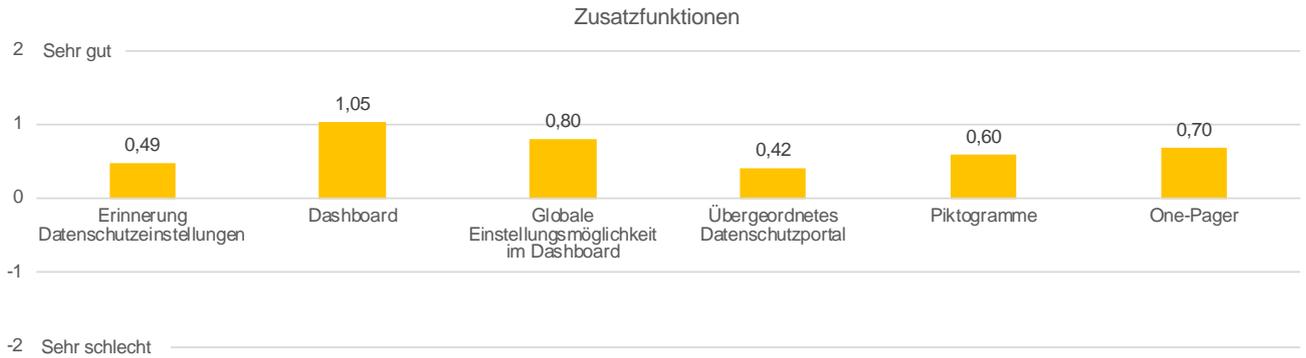


Abbildung 57: Befragungsergebnisse zu Zusatzfunktionen

Hinweise: Die konkreten Fragestellungen finden sich im Anhang A. Anzahl der Observationen zwischen N=1.852 und 1.985.

4.4. Weitere Ergebnisse

Wie in der Bestandsaufnahme diskutiert, gibt es unabhängig von Einstellungsmöglichkeiten auch unterschiedliche Zeitpunkte, zu denen Informationen zur Datenverarbeitung und zum Datenschutz angezeigt werden können. Hierzu zählt bspw. der Anzeigzeitpunkt der Datenschutzerklärung. In den untersuchten Modellen wurden die Informationen zur Datenverarbeitung erst bei der Anmeldung angezeigt, bspw. als Link, also kurz bevor die tatsächliche Verarbeitung stattfindet. Es wäre jedoch auch denkbar, dass Datenschutzinformationen bereits beim ersten Besuch der Webseite dargeboten werden, d.h. die Informationen stehen vor dem Beginn eines Anmeldeprozesses zur Verfügung und könnten so ggf. auch die Nutzungsentscheidung beeinflussen.

Die Befragung sah deshalb eine Frage zum Anzeigzeitpunkt der Datenschutxtexte vor. Insgesamt ist das Ergebnis (s. Abbildung 58) eher ausgeglichen. Etwas mehr (55%) der Teilnehmerinnen und Teilnehmer bevorzugen eine frühzeitige Anzeige der Datenschutzinformationen, während 45% die Darbietung der der Informationen erst kurz vor der tatsächlichen Erhebung wünschen.

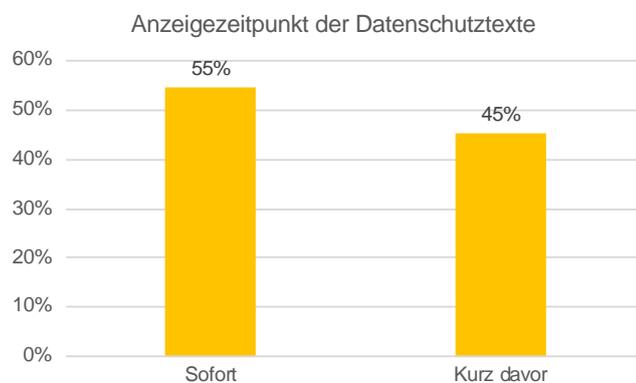


Abbildung 58: Befragungsergebnisse zum Anzeigzeitpunkt der Datenschutxtexte

Hinweise: Die Fragestellung war: „Unabhängig von Einstellungsmöglichkeiten gibt es auch unterschiedliche Zeitpunkte, zu denen Informationen zur Datenverarbeitung und Datenschutz angezeigt werden können. Hierzu zählt bspw. der Anzeigzeitpunkt der Datenschutzerklärung. Zu welchem Zeitpunkt würden Sie diese Informationen gerne erhalten?“ Die Antwortoptionen umfassten „Sofort alles, d.h. in dem Moment, in dem ich auf die Webseite komme“, „Kurz vor dem Zeitpunkt, bevor die jeweilige Datenverarbeitung vorgenommen werden soll“ sowie „Weiß nicht“. Wobei letztere in der Analyse nicht berücksichtigt werden. Die Anzahl der Observationen war N=1.728.

In der Studie von Kettner et al. (2018) war eines der Ergebnisse, dass ein sehr geringer Teil der Verbraucherinnen und Verbraucher Datenschutztexte in der Realität liest. Da dies nicht am mangelnden Interesse an Datenschutzfragen liegen sollte – denn eine Vielzahl von Studien bestätigen, dass Verbraucherinnen und Verbraucher den Datenschutz für ein wichtiges Thema halten – muss es hierfür Gründe geben, die den Datenschutztexten und der Entscheidungssituation zu Grunde liegen. In der Befragung wurden die Teilnehmerinnen und Teilnehmer deshalb gebeten, anzugeben, warum Verbraucherinnen und Verbraucher Datenschutztexte auf Webseiten nicht lesen.²²³

Abbildung 59 fasst die Ergebnisse zusammen und zeigt, welche Gründe die Teilnehmerinnen und Teilnehmer für das Nicht-Lesen von Datenschutztexten nennen. Knapp ein Drittel der Befragten (31%) gibt an, dass der Hauptgrund für das Nicht-Lesen von Datenschutztexten sei, dass das Lesen ohnehin nichts bringt, da man sowieso zustimmen muss. Dieses Empfinden der Befragten deckt sich dabei sehr gut mit den Ergebnissen der Bestandsaufnahme, in der eine große Zahl der Anbieter während des Anmeldeprozesses keine Wahl oder lediglich eine Zustimmung zur Datenverarbeitung vorsah. Auf dem zweiten Rang findet sich mit 24% die Antwortoption, dass das Lesen der Datenschutztexte zu lange dauert. Auch dieses Ergebnis ist im Kontext der Literatur nicht überraschend. So finden Kettner et al. (2018) in ihrem Experiment, dass sich die Lesewahrscheinlichkeit erhöht, wenn Verbraucherinnen und Verbrauchern ein kürzerer Datenschutztext angeboten wird (One-Pager versus Langversion der Datenschutzerklärung).

Mit etwas Abstand folgen die Antwortmöglichkeiten zur Habituation und Gewohnheitseffekten, d.h. dass man sich daran gewöhnt hat, Texte nicht zu lesen (12%). Auch dieses Ergebnis überrascht im Kontext der verhaltenswissenschaftlichen Literatur kaum. So konnte in verschiedenen Studien demonstriert werden, dass sich Gewohnheiten bilden (Thompson & Spencer, 1966) und sich bspw. Sicherheitswarnungen am Computer abnutzen (Anderson et al., 2014). Werden Verbraucherinnen und Verbraucher wiederholt mit (ähnlichen) Datenschutztexten konfrontiert, formen sich Gewohnheiten („habits“), die aus einem „Durchklicken“ („click-through-agreement“) und Nicht-Lesen bestehen (Plaut & Bartlett, 2012).

Auf dem vierten Rang mit immerhin noch 11% geben die Befragten an, dass unübersichtliche Texte dafür sorgen, dass Verbraucherinnen und Verbraucher Datenschutztexte nicht lesen. Auch dieses Ergebnis wird häufig in der Literatur als relevanter Faktor benannt (vgl. Kettner et al., 2018).

Weitere Aspekte, die mit der Gestaltung der Datenschutztexte und der Entscheidungssituation zu tun haben, werden als weniger relevant bewertet.

²²³ Die Bewertung bezog sich dabei auf das Nicht-Lesen „anderer“ Verbraucherinnen und Verbraucher, um soziale Erwünschtheit in Bezug auf die eigene Person zu vermeiden und eine allgemeine Einschätzung des Verbraucherverhaltens zu erhalten.



Abbildung 59: Befragungsergebnisse zum mangeldeln Leseverhalten von Verbraucherinnen und Verbrauchern

Hinweise: Die Fragestellung war: „Können Sie sich vorstellen, warum andere Verbraucherinnen und Verbraucher Datenschutztexte auf Webseiten nicht lesen? (Bitte wählen Sie die wichtigste Antwort aus.)“. Anzahl der Observationen N=1.907.

Darüber hinaus sah die Befragung eine Frage zu den Nutzerwünschen mit Blick auf die Nutzung von Diensten ohne zusätzliche Datenerfassung vor. Die Ergebnisse in Abbildung 60 zeigen, dass die Mehrheit von 77% der Befragten es wichtig oder sogar sehr wichtig finden, dass sie Dienste auch nutzen können, ohne dass Daten, die über den Dienst hinausgehen, erhoben werden. Lediglich 19% der Befragten sind mit Blick auf dieses Vorgehen indifferent und nur 4% finden es unwichtig oder sehr unwichtig.

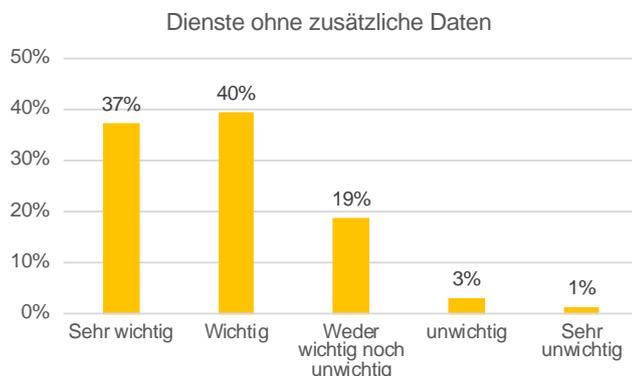


Abbildung 60: Befragungsergebnisse zur Nutzung von Diensten ohne zusätzliche Datenverarbeitung

Hinweise: Die Fragestellung war: „Wie wichtig oder unwichtig ist es für Sie, Dienste im Internet und in der digitalen Welt nutzen zu können, ohne dass über den Dienst hinausgehende Daten von Ihnen erhoben werden (z.B. für Werbezwecke)?“ Anzahl der Observationen N=1.948.

Eine weitere Frage im Fragebogen bezog sich auf das Kopplungsverbot. Hierfür wurden die Teilnehmerinnen und Teilnehmer gefragt, wie problematisch oder unproblematisch sie es bewerten würden, wenn Dienste im Internet nur genutzt werden können, wenn in Datenverarbeitungen, die nicht erforderlich sind, eingewilligt wird. Auch hier sind die Ergebnisse eindeutig (vgl. Abbildung 61). So gaben 70% der Befragten an, dass sie ein solches Vorgehen problematisch oder sogar sehr problematisch fänden. Ein knappes Viertel (24%) standen diesem Vorgehen eher indifferent gegenüber (weder problematisch noch unproblematisch) und 7% gaben an, das Vorgehen als unproblematisch oder sehr unproblematisch zu bewerten.

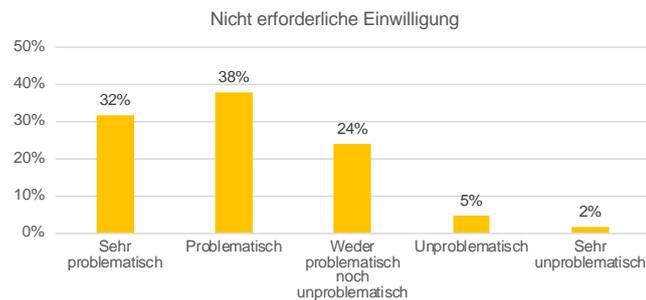


Abbildung 61: Befragungsergebnisse zur Einwilligung in nicht erforderliche Daten

Hinweise: Die Fragestellung war: „Viele Dienste im Internet können nur genutzt werden, wenn Sie in Datenverarbeitungen einwilligen, obwohl diese für den Dienst nicht erforderlich sind (z.B. für Werbezwecke). Wie problematisch oder unproblematisch finden Sie das?“ Anzahl der Observationen N=1.928.

5. Praxistests

Wie bereits in Abschnitt 1.3.6 beschrieben, fanden im Februar und April 2020 zwei Praxistests bei den Forschungspartnern Miele und Telekom statt. Ziel der Praxistests war es, zu überprüfen, wie die entwickelten Einwilligungsmodelle in der Praxis abschneiden und ob diese die Einwilligungssituation der Verbraucherinnen und Verbraucher tatsächlich verbessern. Im Rahmen der Praxistests wurden deshalb Einwilligungsmodelle präsentiert und durch reale Kundinnen und Kunden bewertet, ob die Modelle die Erwartungen und Bedürfnisse an ein Einwilligungsmanagement-System erfüllen.

Dabei unterscheiden sich die beiden Praxistests mit Blick auf zwei Aspekte:

- **Zeitpunkt der Einwilligung und des Managements:** Das erste Modell (Miele) bezog sich dabei rein auf den Einwilligungsprozess bei der erstmaligen Anmeldung in einem Nutzerkonto und den zugehörigen Einwilligungen. Das zweite Modell (Telekom) fokussierte auf das Einwilligungsmanagement im Nachhinein mit einem Datenschutz-Cockpit.
- **Nutzergruppen, an denen das Modell getestet wurde:** Das erste Modell (Miele) wurde an einer selektierten Nutzergruppe in der sog. MyMiele-Community getestet und beschränkt sich auf N=37 Kundinnen und Kunden, die regelmäßig Feedback zu Miele-Produkten geben. Das zweite Modell (Telekom) wurde in einem breiteren Rahmen in einem Online-Panel an N=906 Kundinnen und Kunden getestet. Dieses Online-Panel wird dabei von einem externen Dienstleister verwaltet, der neben dieser Befragung auch noch für weitere Unternehmen Testungen übernimmt.

Detaillierte Informationen zu den getesteten Modellen und den befragten Gruppen finden sich in den Abschnitten 5.1 und 5.2.

5.1. Praxistest „Einwilligung“ (Miele)

Wie bereits erwähnt, wurde der Praxistest bei Miele im Kontext der Einwilligung bei der Erstanmeldung in ein Nutzerkonto durchgeführt. Teilnehmerinnen und Teilnehmer des Praxistests waren Mitglieder der **MyMiele-Community**, d.h. selektierte Kundinnen und Kunden, die regelmäßig zu Feedback zu Unternehmensprodukten befragt werden.

Insgesamt liegen N=37 vollständige Observierungen vor. Dementsprechend sind die Ergebnisse nicht repräsentativ für die deutsche Bevölkerung, sondern decken lediglich einen Teilausschnitt, nämlich ausgewählte Kundinnen und Kunden der Firma Miele, ab.

Im **ersten Schritt** des Praxistests wurde den Kundinnen und Kunden das Einwilligungsmodell in Form von **Mock-Ups** präsentiert. Diese Mock-Ups leiten sich aus dem vorläufigen Anforderungskatalog an ein innovatives Einwilligungsmodell ab und wurden im Workshop mit Vertreterinnen und Vertretern aus Politik, Aufsichtsbehörden, Wirtschaft, Verbänden, Wissenschaft und Zivilgesellschaft validiert (vgl. Abschnitt 1.3.5). Die getesteten Mock-Ups finden sich im Anhang B.

Dabei wurde ein **(fiktiver) Anmeldeprozess** präsentiert, der die Dateneingabe berücksichtigte und hiernach **differenzierte Einstellungsmöglichkeiten** zur Datenverarbeitung erlaubte. Insgesamt sah das Modell vor, dass Kundinnen und Kunden zwischen fünf verschiedenen, Miele-spezifischen Verarbeitungsarten und -zwecken wählen konnten. Hierzu zählten (i) personalisierte Werbung, (ii) Umfragen, (iii) Marktforschung, (iv) Smart-Home-Daten und (v) Verwendung von Geräteinformationen. Das Modell sah dabei datensparsame Voreinstellungen vor und erläuternde Hinweise zu den einzelnen Datenverarbeitungen konnten über Pop-Ups angezeigt werden.

Im **zweiten Schritt** wurden die Kundinnen und Kunden gebeten, das Modell in einem **Fragebogen** zu bewerten. Die Dimensionen zur Bewertung leiten sich – so wie auch in der Nutzerbefragung (Kapitel 4) – aus der wissenschaftlichen Literatur zum HCD und der Forschung zur UX ab. Dabei wurden (i) die Gesamtbewertung des Modells, (ii) die Anpassungsmöglichkeiten, (iii) das Vertrauen in den Anbieter, (iv) die Informiertheit durch die Nutzung des Modells und (v) die Einfachheit der Benutzung berücksichtigt.²²⁴ Zusätzlich wurde eine Frage zur potentiellen Nutzung im Rahmen der Funktionalitäten des Modells ergänzt. Die vollständigen Fragen aus dem nachgeschalteten Fragebogen finden sich im Anhang B.

5.1.1. Einwilligungmodell: Gesamtbewertung

Abbildung 62 zeigt die Gesamtbewertung des getesteten Modells. Insgesamt ist die Bewertung sehr positiv. Dabei geben 35% der Befragten an, dass sie das Modell mit „sehr gut“ bewerten, 49% mit „gut“ und 16% mit „weder gut noch schlecht“. Die Bewertung „weniger gut“ sowie „schlecht“ wurde von keinem Kunden bzw. keiner Kundin vergeben.

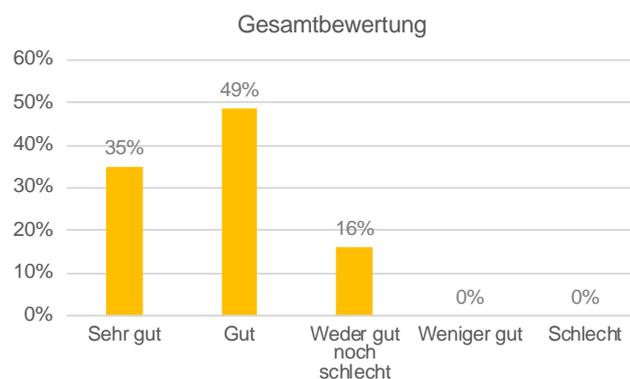


Abbildung 62: Ergebnis Praxistest "Einwilligung" zur Gesamtbewertung des Modells

Hinweise: Die Fragestellung war „Wie beurteilst Du das neue Miele Datenschutz-Management insgesamt?“. Anzahl der Observationen N=37.

Vergleicht man die Bewertung des Miele-Modells mit der Bewertung des Modells v3 aus der Nutzerbefragung, welches dem Miele-Modell am ähnlichsten ist, so stellt man fest, dass die durchschnittliche Bewertung im Miele-Modell insgesamt

²²⁴ Die Fragen waren zu großen Teilen deckungsgleich mit denen der Nutzerbefragung. An wenigen Stellen wurden Antwortoptionen minimal angepasst. Außerdem wurde die Frage zur Übersichtlichkeit des Modells nicht abgefragt, um die Befragungszeit zu reduzieren. Weitere Informationen zu den verwendeten Formulierungen finden sich im Anhang B.

sogar noch höher ausfällt.²²⁵ Die Ergebnisse zur Gesamtbewertung lassen sich wie folgt zusammenfassen:

1. *Das Miele-Modell schneidet mit Blick auf die Gesamtbewertung gut bis sehr gut bei den Kundinnen und Kunden ab.*

5.1.2. Einwilligungsmo­dell: Anpassungsmöglichkeiten

Die Bewertung der Anpassungsmöglichkeiten des Modells findet sich in Abbildung 63. So geben 41% der Kundinnen und Kunden an, dass Sie „voll und ganz zustimmen“, dass das Modell ermöglicht, die Einstellungen an individuelle Bedürfnisse und Anforderungen anzupassen. Weitere 49% „stimmen zu“ und 11% stimmen weder zu noch lehnen ab. Darüber hinaus lehnt kein Kunde bzw. keine Kundin die Aussage ab (0%).

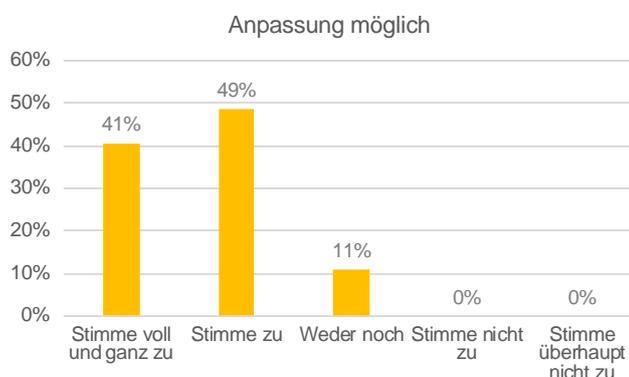


Abbildung 63: Ergebnis Praxistest "Einwilligung" zur Anpassungsmöglichkeit des Modells

Hinweise: Die Fragestellung war „Inwieweit stimmst du der folgenden Aussage zu: Die Gestaltung des neuen Miele Datenschutz-Managements bietet mir die Möglichkeit, diverse Einstellungen an meine individuellen Bedürfnisse und Anforderungen anzupassen“. Anzahl der Observationen N=37.

Auch im Vergleich zum Modell v3 aus der Nutzerbefragung schneidet das Miele-Modell besser ab.²²⁶

Neben der Bewertung der Anpassungsmöglichkeiten wurde im Praxistest eine weitere Frage zu den Einstellungsmöglichkeiten gestellt. Hierbei wurden Kundinnen und Kunden gebeten, zu bewerten, ob die Einstellungsmöglichkeiten im Modell eine Verbesserung für sie darstellen. Die Ergebnisse sind in Abbildung 64 dargestellt. Die große Mehrheit der Kundinnen und Kunden (92%) bejaht dabei, dass das Miele Modell mit Blick auf die Einstellungsmöglichkeiten eine Verbesserung darstellt. Lediglich 8% geben an, dass dies keine Verbesserung darstellen würden.

²²⁵ Das Modell v3 erhält – nach Normierung auf die Skala +2 bis -2 – einen Durchschnittswert von 0,87. Das Miele-Modell hat einen Wert von 1,19. Diese Unterschiede zwischen den beiden Modellen aus Nutzerbefragung und Praxistest sollten jedoch nicht statistisch interpretiert werden und dienen lediglich als Anhaltspunkt für die Performance der Modelle. Zum einen, da die Modelle sich lediglich ähneln, jedoch nicht deckungsgleich sind, zum anderen, weil die Studienpopulationen, d.h. deutsche Bevölkerung versus selektierte Kundinnen und Kunden, sich unterscheiden.

²²⁶ Auch hier gelten die bereits genannten Einschränkungen zur statistischen Vergleichbarkeit. Das Modell v3 aus der Nutzerbefragung erhält als Durchschnittswert 0,58 und das Miele-Modell einen Wert von 1,30.

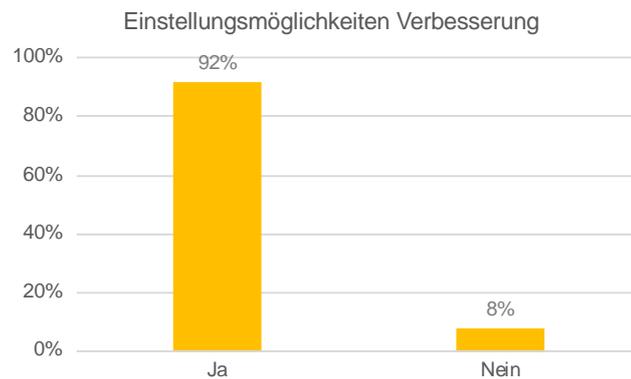


Abbildung 64: Ergebnis Praxistest "Einwilligung" zur Bewertung der Einstellungsmöglichkeiten des Modells

Hinweise: Die Fragestellung war „Im neuen Miele Datenschutz-Management kannst du Einstellungen zu Marketing & Werbung, Deiner Meinung (Umfragen) und Geräteinformationen vornehmen und so die Datennutzung wunschgemäß anpassen. Dies ist bisher noch nicht möglich. Sind diese neuen Einstellungsmöglichkeiten aus deiner Sicht eine Verbesserung?“. Anzahl der Observations N=37.

Zusätzlich zur Abfrage der Zustimmung wurden die Kundinnen und Kunden dazu befragt, wie sie ihre Zustimmung bzw. Ablehnung begründen. Hierzu konnten sie offene Antworten in Textfelder eintragen. Für die Kundinnen und Kunden, die in den Einstellungsmöglichkeiten eine Verbesserung sehen, sind folgende Antworten hervorzuheben:

16 x persönliche Einstellungen möglich

8 x Einfach / Übersichtlich / Verständlich

1 x zeitgemäß

1 x mehr Sicherheit

1 x ... aber man muss sich dafür Zeit nehmen

Bei den Kundinnen und Kunden, die in den Einstellungsmöglichkeiten keine Verbesserung sehen, wurden keine weiteren Erläuterungen zu dieser Bewertung abgegeben.

Die Ergebnisse zu den Einstellungsmöglichkeiten lassen sich wie folgt zusammenfassen:

1. *Die Kundinnen und Kunden stimmen zu, dass das Miele-Modell individuelle Anpassungen ermöglicht.*
2. *Die große Mehrheit der Kundinnen und Kunden sieht die Anpassungsmöglichkeiten im Miele-Modell als eine Verbesserung.*

5.1.3. Einwilligungmodell: Vertrauen in den Anbieter

In Abbildung 65 sind die Ergebnisse zur Bewertung der Vertrauenswürdigkeit des Modells dargestellt. 32% der Kundinnen und Kunden geben dabei an, dass sie „voll und ganz“ zustimmen, dass das Modell vertrauenswürdig ist. 51% stimmen zu und 16% stimmen weder zu noch lehnen ab. Kein Kunde bzw. keine Kundin gibt an, dass sie das Modell als nicht vertrauenswürdig bewerten (0%).

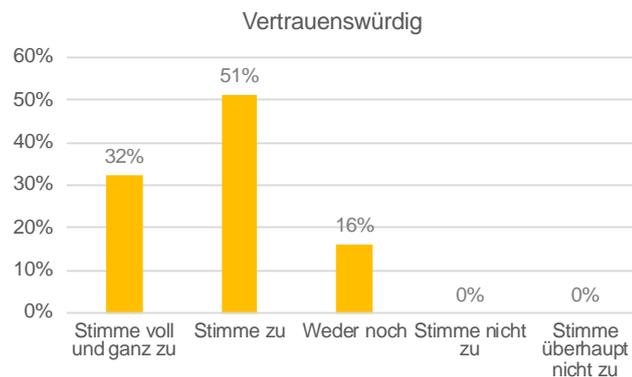


Abbildung 65: Ergebnis Praxistest "Einwilligung" zur Vertrauenswürdigkeit des Modells

Hinweise: Die Fragestellung war „Glaubst du, dass das neue Miele Datenschutz-Management vertrauenswürdig ist?“. Anzahl der Observationen N=37.

Im Vergleich zur Bewertung des Modells v3 in der Nutzerbefragung schneidet das Miele-Modell insgesamt besser ab.²²⁷ Die Ergebnisse lassen sich wie folgt zusammenfassen:

1. *Das Miele-Modell wird von den Kundinnen und Kunden als vertrauenswürdig bewertet.*

5.1.4. Einwilligungsmo­dell: Informiertheit

Die Bewertungen im Hinblick auf die Informiertheit finden sich in Abbildung 66. Insgesamt geben 27% der Kundinnen und Kunden an, dass sie sich „sehr gut“ durch das Modell informiert fühlen. Weitere 49% geben an, sich „gut“ informiert zu fühlen und 22%, dass sie sich „weder gut noch schlecht“ informiert fühlen. Lediglich 3% der Kundinnen und Kunden geben an, sich „nicht gut“ informiert zu fühlen und kein Kunde bzw. keine Kundin (0%) gibt an sich „überhaupt nicht gut“ informiert zu fühlen.

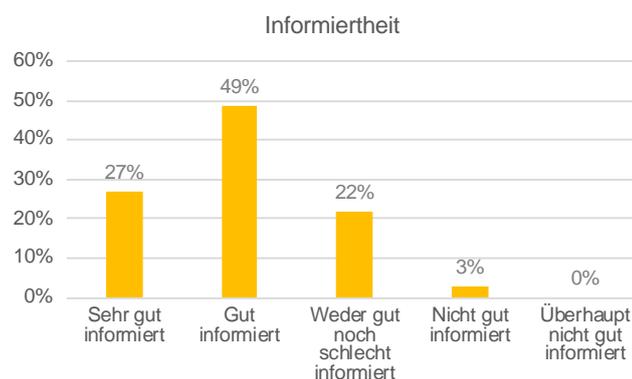


Abbildung 66: Ergebnis Praxistest "Einwilligung" zur Informiertheit durch das Modell

Hinweise: Die Fragestellung war „Wie informiert fühlst du dich nach Nutzung des neuen Miele Datenschutz-Management darüber, wie Miele mit deinen Daten umgeht?“. Anzahl der Observationen N=37.

²²⁷ Die Durchschnittsbewertung von Modell v3 liegt bei 0,63 und beim Miele-Modell bei 1,16. Hierbei gelten weiterhin die statistischen und methodischen Einschränkungen zur Vergleichbarkeit, die bereits erwähnt wurden.

Im Vergleich zum Modell v3 in der Nutzerbefragung schneidet das Miele-Modell damit durchschnittlich besser ab.²²⁸

Die Kundinnen und Kunden, die angaben, sich nicht gut durch das Modell informiert zu fühlen, wurden zusätzlich gebeten, diese Antwort zu begründen. Hierbei gab lediglich eine befragte Person eine Begründung ab. Diese lautete wie folgt:

„Ort, Zweck, Art und Dauer der Speicherung unklar, ebenso fehlt die Info, wie die Nutzerdaten gesichert sind/werden.“

Zusammenfassend lässt sich feststellen:

1. Das Miele-Modell schneidet im Hinblick auf die Informiertheit gut ab.

5.1.5. Einwilligungsmo­dell: Einfachheit

Die Bewertung der Einfachheit des Modells findet sich in Abbildung 67. 32% der Kundinnen und Kunden geben dabei an, dass sie das Modell insgesamt „sehr einfach“ finden. Weitere 41% bewerten es mit „einfach“ und 19% mit „weder einfach noch kompliziert“. 5% geben die Bewertung „kompliziert“ ab und 3% „sehr kompliziert“.

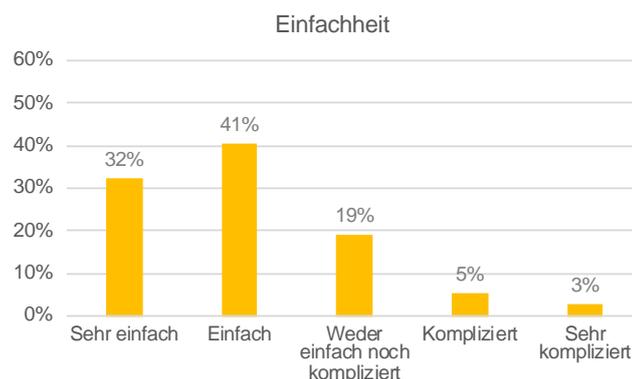


Abbildung 67: Ergebnis Praxistest "Einwilligung" zur Einfachheit des Modells

Hinweise: Die Fragestellung war „Wie einfach oder kompliziert findest Du das neue Miele Datenschutz-Management?“. Anzahl der Observationen N=37.

Insgesamt schneidet das Miele-Modell damit im Vergleich zum Modell v3 aus der Nutzerbefragung ähnlich ab.²²⁹

Die Kundinnen und Kunden (8%), die das Modell als „kompliziert“ oder „sehr kompliziert“ bewertet haben, wurden zusätzlich gebeten, diese Bewertung zu begründen. Eine Antwort war dabei:

„Unnötige Differenzierung zwischen Umfrage und Marktforschung bzw. Smart Home und Geräteinformationen. Wenn ich keine Daten übermitteln will, dann will ich das bei keinem meiner Geräte, ebenso wenn ich keine Befragung durchführen will.“

²²⁸ Die durchschnittliche Bewertung des Modells v3 aus der Nutzerbefragung liegt bei 0,71, während das Miele-Modell eine Durchschnittsbewertung von 1,00 erhält. Auch hier gelten jedoch wieder die Einschränkungen zur Vergleichbarkeit der Modelle.

²²⁹ Das Modell v3 aus der Befragung erhält dabei einen Durchschnittswert von 0,96 und das Miele-Modell von 0,95. Auch hier gelten die bereits erwähnten Einschränkungen zur Vergleichbarkeit.

Die Ergebnisse zur Einfachheit des Modells lassen sich wie folgt zusammenfassen:

1. *Das Miele-Modell wird insgesamt als eher einfach bewertet.*

5.1.6. Einwilligungsmo­dell: Potentielle Nutzung

Neben den unterschiedlichen Bewertungsdimensionen zum Abschneiden des Modells wurden die Kundinnen und Kunden außerdem befragt, ob sie das Miele Datenschutz-Management in der Realität nutzen würden, um bspw. Voreinstellungen anzupassen. Die Ergebnisse finden sich in Abbildung 68. Die große Mehrheit der Befragten (79%) gibt dabei an, dass sie die Funktionalitäten des Modells nutzen würden. Hiervon geben 41% an, dass Modell in der Realität „mit Sicherheit“ zu nutzen und 38% „wahrscheinlich“ zu nutzen. 22% der Kundinnen und Kunden sind unentschlossen und kein Kunde bzw. keine Kundin gibt an, dass sie das Modell nicht nutzen würden, sollte es angeboten werden.

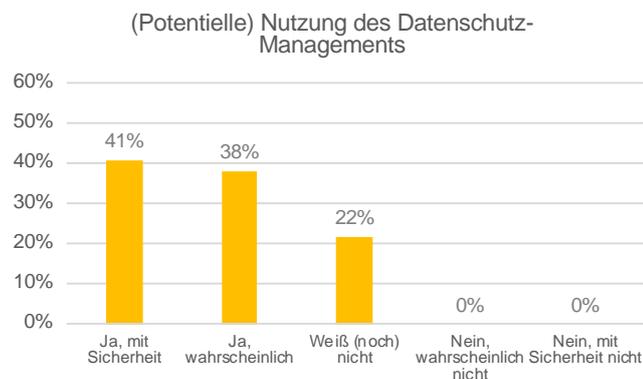


Abbildung 68: Ergebnis Praxistest "Einwilligung" zur potentiellen Nutzung des Modells

Hinweise: Die Fragestellung war „Wenn es das neue Miele Datenschutz-Management in der Realität bereits gäbe, würdest du es dann nutzen?“. Anzahl der Observationen N=37.

Die Ergebnisse lassen sich folgendermaßen zusammenfassen:

1. *Die Mehrheit der Kundinnen und Kunden würde das Modell nutzen, sollte es in der Realität angeboten werden.*

5.1.7. Zusammenfassung

Insgesamt zeigt der Praxistest, dass das Miele-Einwilligungsmodell über alle Bewertungsdimensionen durchweg positiv von den Kundinnen und Kunden bewertet wird. Es ist dabei hervorzuheben, dass insbesondere die angebotenen Anpassungsmöglichkeiten entlang der Differenzierungsdimensionen eine Verbesserung für die Kundinnen und Kunden darstellen. Gefragt nach einer möglichen Nutzung eines solchen Einwilligungsmo­dells und seiner Funktionalitäten in der Realität gibt eine große Mehrheit an, dass sie einer Nutzung positiv gegenüber eingestellt ist.

Bei der Interpretation ist jedoch notwendig zu berücksichtigen, dass sich die Ergebnisse lediglich von einem Teilausschnitt der deutschen Bevölkerung ableiten. So nahmen am Praxistest lediglich Kundinnen und Kunden der Firma Miele teil, die bereits in der Vergangenheit Feedback zu Miele-Produkten gegeben haben.

5.2. Praxistest „Einwilligungsmanagement in Nachhinein“ (Telekom)

Im Praxistest bei der Telekom wurde das Management der Datenverarbeitung im Nachhinein untersucht. Die Anwendungsoberfläche zum Anpassen der Einwilligung im Nachhinein, wurde dabei in einem gesonderten Bereich, dem Telekom „**Mein InfoService**“ untersucht.²³⁰ Aktuell können hier die Datenschutzeinwilligung sowie eine Differenzierung nach Kanal zur Kontaktaufnahme (Telefonnummer, Mail-Adresse und Mobilfunknummer) eingestellt werden. Perspektivisch soll den Kundinnen und Kunden jedoch ein sog. Datenschutz-Cockpit angeboten werden, das eine Differenzierung über weitere Datenarten und Verarbeitungszwecke ermöglicht. Entsprechend wurde dieses Datenschutz-Cockpit im Praxistest auf seine Wirksamkeit untersucht.

Die Daten wurden in einer Befragung in einem aktiv gemanagten **Online-Panel** erhoben. Hierbei wurden lediglich Kundinnen und Kunden der Telekom befragt. Insgesamt liegen N=906 Observationen vor. Diese decken dabei eine breite Bevölkerung ab, können jedoch nicht als repräsentativ für die Gesamtbevölkerung gesehen werden.

In der Testung wurden **zwei unterschiedliche Modelle** (Status Quo versus Datenschutz-Cockpit) gegeneinander getestet. Diese werden in den folgenden Abschnitten genauer beschrieben. Bei der Umsetzung des Praxistests wurde den Kundinnen und Kunden dabei die Umsetzung des Modelle innerhalb eines Bestellprozesses in Form von **Mock-Ups** präsentiert. Diese Mock-Ups wurden im Workshop mit Vertreterinnen und Vertretern aus Politik, Aufsichtsbehörden, Wirtschaft, Verbänden, Wissenschaft und Zivilgesellschaft diskutiert und validiert (vgl. Abschnitt 1.3.5).

Im Anschluss an die Präsentation der Mock-Ups wurden Kundinnen und Kunden gebeten, die Modelle in einem **Fragebogen** zu bewerten. Die Dimensionen zur Bewertung leiten sich – so wie auch in der Nutzerbefragung (Kapitel 4) – aus der wissenschaftlichen Literatur zum HCD und der Forschung zur UX ab. Dabei wurden (i) die Anpassungsmöglichkeiten, (ii) das Vertrauen in den Anbieter, (iii) die Übersichtlichkeit und (iv) die Verständlichkeit berücksichtigt.²³¹ Zusätzlich wurde bei der Modellbewertung abgefragt, als wie (v) hilfreich das Modell wahrgenommen wird und ob es (vi) einen Mehrwert für Kundinnen und Kunden darstellt. Die vollständigen Fragen aus dem nachgeschalteten Fragebogen finden sich im Anhang C.

5.2.1. Version A: Status Quo

Das erste Modell stellt den **Status Quo** (Kontrollbedingung) zur Testung dar und zeigt die aktuelle Umsetzung des Datenschutzmanagements im Nachhinein.

²³⁰ Grundsätzlich, d.h. im Normalbetrieb unabhängig vom Praxistest, sind Datenschutzeinstellungen und Einwilligungen im Kundencenter einzusehen und einzustellen.

²³¹ Die Fragen waren zu großen Teilen deckungsgleich mit denen der Nutzerbefragung. An wenigen Stellen, bspw. zur Verständlichkeit, wurde die Fragestellung nebst Antwortoptionen angepasst.

Hierfür wurde den Kundinnen und Kunden der **InfoService** in seiner alten Ausgestaltung angezeigt. In diesem können Kundinnen und Kunden einstellen, welche Daten verarbeitet werden dürfen. Gestalterisch wurden Check-Boxen eingesetzt (vgl. Abbildung 69).



Abbildung 69: Design Praxistest "Einwilligungsmanagement im Nachhinein" - InfoService Status Quo (Version A)

5.2.2. Version B: Erweiterung mit Datenschutz-Cockpit

Die zweite Version, die im Praxistest überprüft wurde, stellt eine Erweiterung der ersten Version dar, bei der ein angepasstes Datenschutzmanagement im Nachhinein zum Einsatz kam.

Hierfür wurde eine Erweiterung bzw. Neugestaltung des Telekom **InfoService** abgebildet, die ein **Datenschutz-Cockpit** darstellt und die erteilten Einwilligungen im Hinblick auf die Datenverarbeitung feingranular ermöglicht. Einstellungen können im Cockpit mit Schiebereglern angepasst werden und es wird über unterschiedliche Datenarten differenziert (Abbildung 70).



Abbildung 70: Design Praxistest „Einwilligungsmanagement im Nachhinein“ – Neuer InfoService als Datenschutz-Cockpit (Version B)

5.2.3. Überblick über die Bewertung und Vergleich beider Modelle

Abbildung 71 zeigt die Ergebnisse der Bewertung der beiden Modelle an. Die graue Linie markiert dabei die Bewertungen von Version A (Status Quo), also dem alten Einwilligungsmanagement. Die gelbe Linie zeigt die Bewertungen von Version B (Datenschutz-Cockpit) an, also dem neuen Einwilligungsmanagement. Die Punkte markieren jeweils die Zustimmung zu den einzelnen Bewertungsdimensionen, nämlich die (i) die Anpassungsmöglichkeiten, (ii) das Vertrauen in den Anbieter, (iii) die Übersichtlichkeit und (iv) die Verständlichkeit, (v) wie hilfreich das Modell wahrgenommen wird und ob es (vi) einen Mehrwert für die Kundinnen und Kunden bietet.

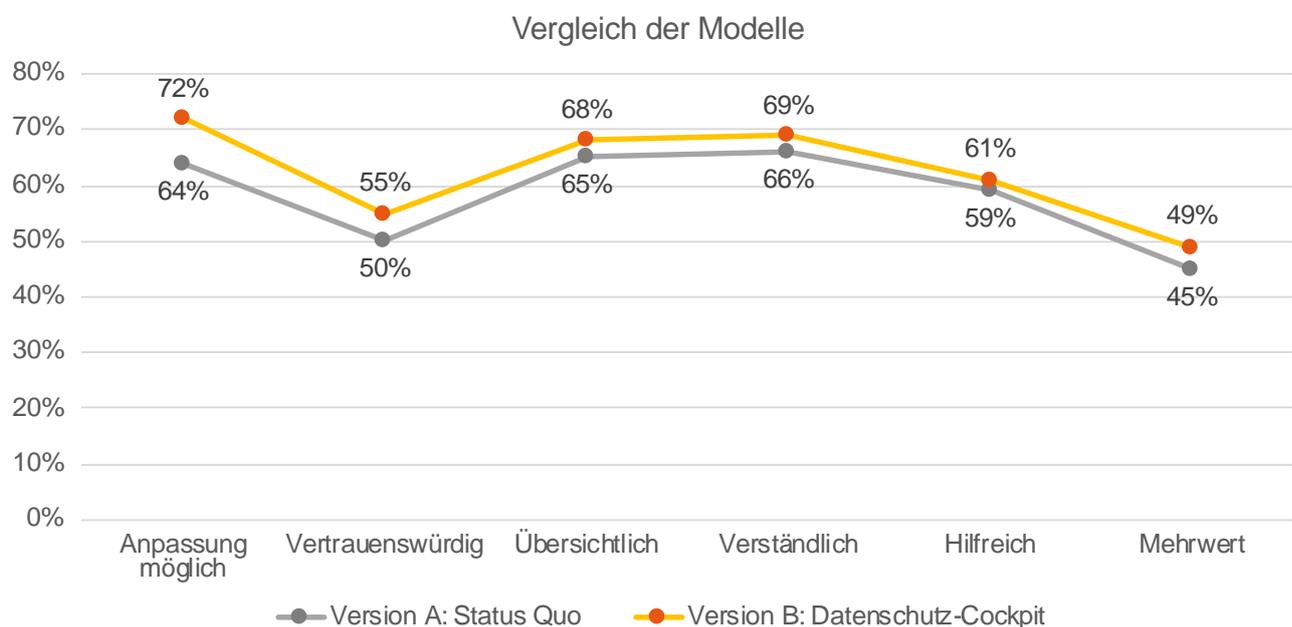


Abbildung 71: Ergebnis Praxistest „Einwilligungsmanagement im Nachhinein“ zum Überblick über die Bewertung und Vergleich der Modelle

Hinweise: Die Prozentzahl gibt die Zustimmung zu den jeweiligen Bewertungsdimensionen an. Die konkreten Fragestellungen finden sich in Anhang C. Anzahl der Observationen N=906.

Unabhängig vom Modell zeigen die Ergebnisse, dass das Einwilligungsmanagement im Nachhinein von den Kundinnen und Kunden durchweg positiv bewertet wird. Dabei schneiden die Modelle in einigen Bewertungsdimensionen besser ab als in anderen. Darüber hinaus kann festgestellt werden, dass Version B, also das Datenschutz-Cockpit, in allen Bewertungsdimensionen besser als Version A (Status Quo) bewertet wird. Die Unterschiede reichen dabei von 2% bis 8%.

Im Folgenden wird auf die Einzeldimensionen eingegangen und hiernach die Ergebnisse zusammengefasst.

5.2.4. Nutzung des InfoService: Anpassungsmöglichkeiten

Die Bewertung der Anpassungsmöglichkeiten der beiden InfoService-Versionen sind insgesamt sehr gut. Version A (Status Quo) erhält in der Bewertung durch die Kundinnen und Kunden eine Zustimmungsrate von 64%. Version B (Daten-

schutz-Cockpit) erreicht eine Zustimmungsrate von 72%. Der Unterschied zwischen den beiden Versionen deutet darauf hin, dass Version B insgesamt besser beurteilt wird, auch wenn aus den Daten keine statistische Aussagekraft für die Ergebnisse abgeleitet werden kann.²³²

Zusammenfassend kann festgehalten werden:

1. *Beide Telekom-Modelle erhalten insgesamt gute Bewertungen für die Anpassungsmöglichkeiten.*
2. *Das Datenschutz-Cockpit wird mit Blick auf die Anpassungsmöglichkeiten aus Sicht der Kundinnen und Kunden besser bewertet als das Status-Quo-Modell.*

5.2.5. Nutzung des InfoService: Vertrauen in den Anbieter

Auch das Vertrauen in den Anbieter ist mit Blick auf die beiden Modelle als positiv zu bewerten. Version A (Status Quo) erhält von der Hälfte der Befragten (50%) die Zustimmung, dass die Ausgestaltung vertrauenswürdig ist. Für Version B (Datenschutz-Cockpit) liegt die Zustimmungsrate mit 55% sogar noch höher. Der Unterschied zwischen beiden Versionen kann zwar nicht statistisch interpretiert werden, jedoch deutet die Tendenz darauf hin, dass Version B im Vergleich zu Version A besser bei den Kundinnen und Kunden ankommt.

Zusammenfassend lässt sich feststellen:

1. *Beide Telekom-Modelle werden mit Blick auf die Vertrauenswürdigkeit des Anbieters positiv bewertet.*
2. *Die Vertrauenswürdigkeit des Modells mit Datenschutz-Cockpit ist aus Sicht der Kundinnen und Kunden größer als beim Status-Quo-Modell.*

5.2.6. Nutzung des InfoService: Übersichtlichkeit

Auch mit Blick auf die Übersichtlichkeit der Modelle werden gute Werte erreicht. So stimmen bei Version A (Status Quo) 65% der Kundinnen und Kunden zu, dass das Modell übersichtlich und klar ist. Einen ähnlichen, leicht höheren Wert, erhält mit 68% Version B (Datenschutz-Cockpit). Auch hier kann in der Tendenz – nicht jedoch in der statistischen Beurteilung – ein besserer Wert durch Version B erzielt werden.

Die Ergebnisse zur Übersichtlichkeit der Modelle lassen sich, wie folgt, zusammenfassen:

1. *Mit Blick auf die Übersichtlichkeit erzielen beide Telekom-Modelle positive Bewertungen.*
2. *Das Datenschutz-Cockpit erhält in der Tendenz bessere Bewertungen als das Status-Quo-Modell.*

²³² Das bedeutet, dass eine Berechnung von Signifikanzen und Effektstärken aufgrund der Datengrundlage nicht möglich ist und die Ergebnisse somit nicht hierhingehend interpretiert werden sollten. Dieser Hinweis gilt auch für die Interpretation der Unterschiede in den folgenden Abschnitten.

5.2.7. Nutzung des InfoService: Verständlichkeit

Die Verständlichkeit der beiden Modelle ist ebenfalls sehr zufriedenstellend. So stimmen 66% der Kundinnen und Kunden zu, dass Version A (Status Quo) verständlich ist. Version B (Datenschutz-Cockpit) erzielt mit 69% einen leicht besseren Wert. Auch dieser Unterschied sollte nicht statistisch interpretiert werden, jedoch weisen die Daten darauf hin, dass das Datenschutz-Cockpit etwas besser bewertet wird.

Zusammenfassend kann festgestellt werden:

1. *Beide Telekom-Modelle erreichen sehr gute Bewertungen bei der Verständlichkeit.*
2. *Das Datenschutz-Cockpit erzielt dabei eine minimal bessere Bewertung als das Status-Quo-Modell.*

5.2.8. Nutzung des InfoService: Hilfe

Die Bewertung der Kundinnen und Kunden inwieweit die beiden Modelle hilfreich sind, fällt ebenfalls gut aus. So stimmen 59% zu, dass Version A (Status Quo) insgesamt eine Hilfe für sie darstelle. Bei Version B (Datenschutz-Cockpit) liegt die Zustimmungsrate bei 61%. Somit schneidet auch in diesem Fall Version B leicht besser als Version A ab.

Die Ergebnisse im Hinblick auf die Bewertungsdimension „Hilfe“ lassen sich entsprechend zusammenfassen:

1. *Sowohl das Status-Quo-Modell als auch das Datenschutz-Cockpit wird von Kundinnen und Kunden mehrheitlich als hilfreich bewertet.*
2. *Das Datenschutz-Cockpit schneidet dabei leicht besser als das Status-Quo-Modell ab.*

5.2.9. Nutzung des InfoService: Mehrwert

Die Bewertung des Mehrwerts der Modelle für Kundinnen und Kunden fallen im Vergleich zu den anderen Bewertungsdimensionen am schlechtesten aus, sind jedoch zufriedenstellend. So stimmen 45% der Kundinnen und Kunden, die zu Version A (Status Quo) befragt wurden zu, dass das Modell ihnen einen Mehrwert biete. Bei Version B (Datenschutz-Cockpit) ist die Zustimmungsrate mit 49% etwas höher. Auch hier lässt sich zumindest eine Tendenz erahnen, dass Version B besser ist als Version A.

Zusammenfassen lässt sich feststellen:

1. *Beide Telekom-Modelle erhalten im Hinblick auf den Mehrwert annehmbare, tendenziell positive, Werte.*
2. *Das Datenschutz-Cockpit schneidet dabei besser als das Status-Quo-Modell ab.*

5.2.10. Zusammenfassung

Insgesamt konnte der Praxistest zum Datenschutzmanagement im Nachhinein zeigen, dass das eine solche Funktion positiv von Kundinnen und Kunden bewertet wird. Dabei sollte berücksichtigt werden, dass nur wenige andere Anbieter eine solche Funktion überhaupt anbieten (vgl. Abschnitt 2.2.1.3) und somit sowohl das Status-Quo-Modell als auch das Datenschutz-Cockpit eine Verbesserung für Kundinnen und Kunden darstellt. Mit Blick auf die unterschiedlichen Bewertungsdimensionen trifft dies insbesondere auf die Anpassungsmöglichkeiten, Übersichtlichkeit und Verständlichkeit der beiden Modelle zu.

Diese Ergebnisse unterstreichen den Befund aus der Nutzerbefragung (vgl. Abschnitt 4.3). Hier konnte festgestellt werden, dass ein sog. „Dashboard“, das in seiner Funktionalität äquivalent zum Einwilligungsmanagement im Telekom-Praxistest ist, die besten Bewertungen der Verbraucherinnen und Verbraucher bei den Zusatzfunktionen erhielt.

Vergleicht man die unterschiedlichen Ausgestaltungen, d.h. Status-Quo-Modell mit Text und Check-Boxen und Datenschutz-Cockpit mit Schiebereglern, so weisen die Daten darauf hin, dass zumindest in der Tendenz die Ausgestaltung in einem Datenschutz-Cockpit zu bevorzugen ist.

Bei der Interpretation muss jedoch beachtet werden, dass die Daten lediglich einen Teilausschnitt der Bevölkerung darstellen und im Praxistest lediglich Kundinnen und Kunden der Telekom befragt wurden. Die Befragung bezog sich zwar auf eine realitätsnahe Situation und die Datengrundlage ist mit N=906 komfortabel, dennoch kann hieraus nicht grundsätzlich abgeleitet werden, dass Einwilligungsmanagementsysteme für die Verwaltung von Daten im Nachhinein für alle Verbrauchergruppen gleichermaßen sinnvoll sind.

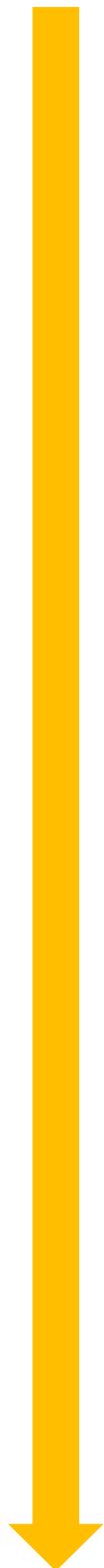
6. Best Practice-Modell

Diese Studie zielt übergeordnet darauf ab aufzuzeigen, wie die Vorgaben der DS-GVO hinsichtlich der Einwilligung sowohl rechtskonform als auch nutzerfreundlich umgesetzt werden können. Hierbei zeigen gerade die Ergebnisse der repräsentativen Online-Befragung sowie der Praxistests bei Miele und der Telekom sehr deutlich, dass dies praktikabel möglich ist und dabei auch die Interessen der Unternehmen angemessen gewahrt bleiben. So befürworten Verbraucherinnen und Verbraucher differenzierte Einwilligungen und datensparsame Voreinstellungen überwiegend sehr deutlich. Und auch die Unternehmen profitieren davon, wenn sie ihren Kundinnen und Kunden einfache und übersichtliche Benutzeroberflächen mit Wahlmöglichkeiten anbieten. Denn Verbraucherinnen und Verbraucher schätzen Anbieter, die differenzierte Einwilligungsmodelle einsetzen, als wesentlich vertrauenswürdiger ein als solche, die dies nicht tun (vgl. Abschnitt 4.1.3).

Im Folgenden werden nun die relevanten Aspekte eines Best Practice-Modells vorgestellt und Umsetzungsschritte zur Implementierung beschrieben, die Unternehmen aufzeigen, wie sie die Vorgaben der DS-GVO rechtskonform und zugleich nutzerfreundlich umsetzen können (vgl. Abschnitte 6.1 bis 6.4). Das Best Practice-Modell bezieht sich sowohl auf die einmalige Einholung einer Einwilligung als auch die Einwilligung bei komplexen Systemen wie z.B. bei den Einstellungen bei einem Betriebssystem, bei einem Browser, bei Nutzung eines "Sozialen Netzwerkes" oder bezogen auf verschiedene Datenverarbeitungsvorgänge eines Unternehmens. Die Modelle einschließlich des Datenschutz-Cockpit werden zusätzlich zur besseren Nachvollziehbarkeit in Mock-Ups – sowohl für Desktop als auch für mobile Endgeräte – verbildlicht (vgl. Abschnitt 6.5).

Inhaltlich wird die Umsetzung dabei für ein fiktives, prototypisches Unternehmen vorgenommen. Das Modell stützt sich dabei auf fünf unterschiedliche Befunde, die in den vorhergegangenen Kapiteln beschrieben wurden: gesetzliche Vorgaben, verhaltenswissenschaftliche Erkenntnisse, die Ergebnisse unserer Verbraucherbefragung, Feedback aus dem Expertenworkshop sowie unseren Praxistests bei zwei Unternehmen.

Das Modell gliedert sich in drei Phasen: von der Vorbereitung, über die Umsetzung des Einwilligungsmodells bis hin zur Umsetzung eines Datenschutz-Cockpits. Überdies könnte das Modell noch um optionale Zusatzfunktionen erweitert werden. Die folgende Abbildung illustriert die Phasen und die mit ihnen korrespondierenden Anforderungen und Umsetzungsschritte. Im Folgenden werden diese Phasen und Anforderungen im Detail erläutert.



<h3>A) Vorbereitungsphase</h3> <p>Anforderung 1: Einwilligungen dürfen nur dann eingeholt werden, wenn sie notwendig sind. Auch sollte der situative Kontext berücksichtigt werden.</p> <p>Anforderung 2: Zwischen unterschiedlichen Verarbeitungsvorgängen ist zu differenzieren.</p> <p>Anforderung 3: Die Differenzierungsmöglichkeiten bei der Einwilligung sollten jedoch dosiert eingesetzt werden. Bei Einwilligungsmanagement-Systemen mit umfangreichen Einwilligungen sollte eine "Entscheidungsbaumlogik" verwendet werden, so dass Nutzerinnen und Nutzer mit möglichst wenig Klicks ihre Datenschutz-Präferenzen einstellen können.</p> <p>Anforderung 4: Auch ohne Einwilligung muss die Nutzung des Dienstes möglich sein.</p>
<h3>B) Umsetzungsphase Einwilligung</h3> <p>Anforderung 5: Insgesamt sollte das Modell einfach bedienbar, nutzergruppenspezifisch gestaltet und mit unterschiedlichen Endgeräten kompatibel sein.</p> <p>Anforderung 6: Informationen zur Datenverarbeitung sollten transparent, verständlich und gestalterisch neutral in das Modell eingebunden werden. Hierbei ist die richtige Dosierung wichtig.</p> <p>Anforderung 7: Für die einwilligungsrelevanten Aspekte muss das Modell datensparsame Voreinstellungen vorsehen.</p> <p>Anforderung 8: Übergeordnet darf das Modell nicht vom Wesentlichen ablenken. Weiterhin ist eine manipulierende Gestaltung oder Framing der Modellinhalte zu unterlassen.</p>
<h3>C) Umsetzungsphase Datenschutz-Cockpit</h3> <p>Anforderung 9: Zur nachträglichen Verwaltung der erteilten Einwilligungen und Datenverarbeitungen sowie zur erleichterten Ausübung von Datenschutz-Nutzungsrechten sollte ein Datenschutz-Cockpit zur Verfügung gestellt werden.</p>
<h3>Optionale Zusatzfunktionen</h3> <p>Anforderung 10: Visualisierungen wie Icons oder Piktogramme können als Hilfestellung für die Verständlichkeit der Datenverarbeitung genutzt werden.</p> <p>Anforderung 11: Eine Erinnerungsfunktion zum Überprüfen der Datenschutzeinstellungen kann das Modell sinnvoll ergänzen.</p>

Fortlaufend in allen Phasen: Testung und juristisches Monitoring

6.1. Vorbereitungsphase (A)

Bevor ein Unternehmen an die Ausgestaltung eines Einwilligungsmanagementsystem geht, sind Vorbereitungsschritte notwendig. Zunächst muss hierbei überprüft werden, ob eine datenschutzrechtliche Einwilligung überhaupt nötig ist. Wenn dies der Fall ist, sind die für das Einwilligungsmanagementsystem relevanten Datenarten und zugehörigen Verarbeitungszwecke zu definieren. Hieraus wird in einem abschließenden Schritt abgeleitet, zu welchen Datenverarbeitungszwecken differenzierte Einwilligungen eingeholt werden müssen.

Im Folgenden werden zunächst hierbei zu berücksichtigende Anforderungen und dann Illustrationen zur Umsetzung dargestellt.

6.1.1. Anforderungen

6.1.1.1. Anforderung 1: Einwilligungen dürfen nur dann eingeholt werden, wenn sie notwendig sind. Auch sollte der situative Kontext berücksichtigt werden.

Aus rechtlicher Perspektive dürfen Einwilligungen für Datenverarbeitungen nur dann eingeholt werden, wenn sie notwendig sind bzw. die Datenverarbeitungen nicht bereits durch andere Tatbestände der DS-GVO gerechtfertigt sind. Das bedeutet, dass Daten verarbeitende Stellen keine Einwilligung benötigen, wenn die Datenverarbeitung zur Vertragserfüllung erforderlich ist (Art. 6 Abs. 1 b) DS-GVO) oder wenn für sie ein berechtigtes Interesse (Art. 6 Abs. 1 f) DS-GVO) besteht. Aus verhaltenswissenschaftlicher Sicht ist das Einholen einer unnötigen Einwilligung ebenfalls problematisch, denn der Akt der Einwilligung könnte eine Wahlfreiheit suggerieren, die in Wirklichkeit nicht existiert (vgl. Abschnitt 2.3.1). Entsprechend sieht das Best Practice-Modell vor, dass lediglich dann eine Einwilligung eingeholt werden darf, wenn sie notwendig ist.

Des Weiteren sollte das Modell den situativen Kontext, d.h. den jeweiligen Zeitpunkt der Datenverarbeitung, beim Einholen der Einwilligung berücksichtigen. Wenn bestimmte Datenverarbeitungen erst zu einem späteren Zeitpunkt relevant sind und nicht zu den „Grundfunktionen“ eines Dienstes zählen, sollte auch die jeweilige Einwilligung erst zu diesem späteren Zeitpunkt eingeholt werden – und nicht pauschal zu Beginn. Dies ist etwa bei komplexen Betriebssystemen der Fall. Anstatt Einwilligungen vorweg für alle möglichen Datenverarbeitungen einzuholen, die jedoch von Nutzerinnen und Nutzern gar nicht genutzt werden, sollten zunächst nur Einwilligungen für die Datenverarbeitungen, die tatsächlich erfolgen, eingeholt werden. Sobald Nutzerinnen und Nutzer im Verlauf weitere Dienste in Anspruch nehmen möchten, für deren Datenverarbeitung noch keine Einwilligung vorliegt, sollte diese zu dem Zeitpunkt – d.h. situativ – eingeholt werden.

6.1.1.2. Anforderung 2: Zwischen unterschiedlichen Verarbeitungsvorgängen ist zu differenzieren.

Das (rechtliche) Gebot der „Granularität“ macht es erforderlich, dass bei Einwilligungen, in denen Daten zu unterschiedlichen Zwecken erhoben werden sollen, für jeden Zweck gesonderte Einwilligungen erforderlich sind. Verbraucherinnen und Verbrauchern sollten dementsprechend Datenverarbeitungen gemäß ihren Präferenzen anpassen können und den Datenverarbeitungen zustimmen, die

sie begrüßen, während sie unerwünschte Datenverarbeitungen ablehnen können. Eine globale Einwilligung, ohne ausreichende Informationen zur Datenverarbeitung und ohne Differenzierungsmöglichkeiten hält hingegen nicht den gesetzlichen Vorgaben stand. Auch die verhaltenswissenschaftliche Literatur bestätigt, dass mangelnde Wahlfreiheit nicht im Interesse der Verbraucherinnen und Verbraucher ist (Abschnitt 2.3.1).

Die Befragungsergebnisse zu den Erwartungen und Bedürfnissen von Verbraucherinnen und Verbrauchern unterstützen die rechtlichen Vorgaben und verhaltenswissenschaftlichen Empfehlung klar (vgl. Abschnitt 4.1). Die Modelle mit Differenzierungsmöglichkeiten schneiden eindeutig besser ab als solche ohne Differenzierungsmöglichkeit. Das Einwilligungsmodell, das eine globale Einwilligung vorsieht, hält dabei den Erwartungen und Bedürfnissen der Verbraucherinnen und Verbraucher nicht stand. So zeigt die Befragung, dass das globale Einwilligungsmodell zwar etwas besser als das Einwilligungsmodell mit erzwungener Einwilligung abschneidet; im Vergleich mit den anderen Modellen, die eine Differenzierung vorsehen, ist die Bewertung aber eindeutig schlechter. In Zahlen bedeutet dies, dass das Modell mit Differenzierung und Pop-Ups von 70% der Befragten als gut oder sogar sehr gut bewertet wird (N=1.024). Das Modell ohne Differenzierung und erzwungener Globaleinwilligung wird hingegen lediglich von 39% der Befragten als gut oder sehr gut bewertet (N=1.012).

Auch der Praxistest zum Einwilligungsmodell bei Miele bestätigt diese Ergebnisse. So bejahen 89% der befragten Kundinnen und Kunden (N=37), dass das Modell Anpassungen an individuelle Bedürfnisse erlaubt. Darüber hinaus gibt eine große Mehrheit von 92% der Kundinnen und Kunden an, dass die angebotenen Anpassungsmöglichkeiten eine Verbesserung darstellen (vgl. Abschnitt 5.1.2)

6.1.1.3. Anforderung 3: Die Differenzierungsmöglichkeiten bei der Einwilligung sollten jedoch dosiert eingesetzt werden. Bei Einwilligungsmanagement-Systemen mit umfangreichen Einwilligungen sollte eine "Entscheidungsbaumlogik" verwendet werden, so dass Nutzerinnen und Nutzer mit möglichst wenig Klicks ihre Datenschutz-Präferenzen einstellen können.

Aus rechtlicher Perspektive mag eine vollständige Differenzierung über Datenarten und (Unter-)Zwecke erforderlich sein. Jedoch zeigt die verhaltenswissenschaftliche Literatur, dass bei einer überbordenden Anzahl von Optionen schnell eine Überforderung der Nutzerinnen und Nutzer eintreten kann. So ist es möglich, dass Einstellungsmöglichkeiten überhaupt nicht genutzt werden (vgl. Abschnitt 2.1.2.2.3).

Die Bedürfnisse der Verbraucherinnen und Verbraucher, die sich aus der Befragung ergeben, sind mit Blick auf die Tiefe der Differenzierung hingegen weniger eindeutig (vgl. Abschnitt 4.2.2). Weder keine, mittlere noch eine starke Differenzierung werden anderen Differenzierungsoptionen klar vorgezogen.

Letztendlich ist es aus Gründen der Nutzerfreundlichkeit ratsam, auf einen vernünftigen, dosierten Grad der Differenzierung zu achten und nur so viele Einzelaspekte zu definieren, wie sie rechtlich erforderlich sind.

Bei komplexeren Datenverarbeitungen, bei denen eine größere Anzahl von Datenarten für eine Vielzahl unterschiedlicher Zwecke verwendet werden sollen (z.B. Einstellungen bei einem Betriebssystem, bei einem Browser, bei Nutzung

eines "Sozialen Netzwerkes" oder bezogen auf verschiedene Datenverarbeitungsvorgänge eines Unternehmens), sind überdies Entscheidungsbaumlogiken zur Abkürzung des Einwilligungsprozesses zu verwenden. Hierdurch werden die Nutzerinnen und Nutzer in die Lage versetzt, schnell zu entscheiden, ob sie überhaupt wollen, dass bestimmte Datenarten für bestimmte Zwecke verwendet werden. Wenn sie dies wollen, hätten sie in einem nächsten Schritt die Möglichkeit, granular zu entscheiden, welche Daten für welche Zwecke verwendet werden dürfen.

6.1.1.4. Anforderung 4: Auch ohne Einwilligung muss die Nutzung des Dienstes möglich sein.

Aus rechtlicher Sicht sind Systeme, bei denen Nutzerinnen und Nutzer nicht ohne Einwilligung (jenseits der Vertragsdurchführung!) den Dienst bzw. das Angebot nutzen können, unzulässig. Gleiches gilt für die Einwilligungen in Newsletter oder Werbeaktivitäten, ohne die Nutzerinnen und Nutzer kein Konto anlegen bzw. den Dienst nicht nutzen können. Die verhaltenswissenschaftliche Bewertung kommt zu einem ähnlichen Schluss: Mangelnde Wahlfreiheit gilt es zu vermeiden und so fällt das Modell mit einer erzwungenen Einwilligung sowohl in der verhaltenswissenschaftlichen Betrachtung als auch in der Verbraucherbefragung auf ganzer Linie durch (vgl. Abschnitt 4.1).

Zusammenfassend bedeutet dies: Nutzerinnen und Nutzer müssen den Dienst auch nutzen können, ohne gezwungen zu werden, eine Einwilligung zu geben. Ohne Einwilligung kann es dann zwar möglich sein, dass bestimmte *zusätzliche* Funktionen nicht genutzt werden können – doch die Nutzung des Dienstes an sich darf hiervon nicht betroffen sein.

6.1.2. Vorbereitungsphase: Illustration der Umsetzung

Die vorgestellten Anforderungen der Vorbereitungsphase sollten wie folgt in die Praxis umgesetzt werden. Hierbei ist zunächst zu definieren, welche Datenverarbeitungen neben denen, die unter das berechnete Interesse fallen, überhaupt existieren. Diese Datenverarbeitungen wären dann relevant für eine Einwilligung und sollten bei der Planung des Modells berücksichtigt werden.

Hierfür ist zu spezifizieren, welche Daten und zu welchem Zweck sie erhoben und verarbeitet werden sollen. Grundsätzlich sind diese Verarbeitungen sehr individuell und müssen an die Bedürfnisse der jeweiligen verarbeitenden Stelle angepasst werden. Wie in Abschnitt 2.1.2.2.7 diskutiert, sind aus Verbraucherperspektive unterschiedliche Datenarten, wie Daten zur Person oder Standortinformationen, sowie vier unterschiedliche Verarbeitungszwecke besonders relevant.

Im Folgenden wird am Beispiel eines fiktiven Unternehmens aufgezeigt, wie die konkreten Umsetzungsschritte vollzogen werden können:

Das fiktive Unternehmen „DS-Leuchtturm AG“ entscheidet, dass es neben der Datenverarbeitung zur Vertragserfüllung folgende Datenarten zu unterschiedlichen Zwecken erheben möchte:

- Daten zur Person, d.h. Name, Alter, Geschlecht, für Werbezwecke und zur Weitergabe an andere Unternehmen

- Webaktivitäten zur Profilbildung
- Gerätekennungen zur Identifikation
- Standortdaten für Werbezwecke und zur Profilbildung

Tabelle 4 fasst diese Aspekte zusammen:

		Zwecke			
		Werbung	Weitergabe an andere Unternehmen	Profilbildung	Identifikation
Datenart	Daten zur Person	X	X		
	Webaktivitäten			X	
	Geräteerkennung				X
	Standortdaten	X		X	

Tabelle 4: Illustration der Umsetzung des Best Practice-Modells – Datenarten und Zwecke

Da diese Aspekte, wie erwähnt, nicht unter das berechtigte Interesse fallen, sind somit einzelne, differenzierte Einwilligungen für die genannten Datenverarbeitungen notwendig.

Wenn weitere Datenverarbeitungen erst zu einem späteren Zeitpunkt relevant werden, dann muss in diese auch erst zu einem späteren Zeitpunkt eingewilligt werden. Auch für diese Datenverarbeitungen muss die Datenart und der zugehörige Zweck definiert werden. Die Umsetzung erfolgt dann analog zu den im folgenden beschriebenen Phasen.

Im Falle von komplexeren Datenverarbeitungen, bei denen eine Vielzahl von Datenarten und Zwecken mit einander kombiniert werden, ist es notwendig, eine mehrstufige Entscheidungsbaum-Logik aufzusetzen. Die erste Stufe unterscheidet dabei zwischen den Datenarten und soll erlauben, dass Nutzerinnen und Nutzer zuerst entscheiden für welche spezifischen Datenarten sie überhaupt Datenschutzeinstellungen vornehmen wollen. Auf Grundlage der Auswahl in der ersten Stufe werden dann in der zweiten Stufe nur die zugehörigen Verarbeitungszwecke angezeigt. Abbildung 72 verbildlicht eine solche Entscheidungsbaumlogik, die, wie angedeutet, um eine Vielzahl weiterer Datenarten und Verarbeitungszwecke erweitert werden kann.

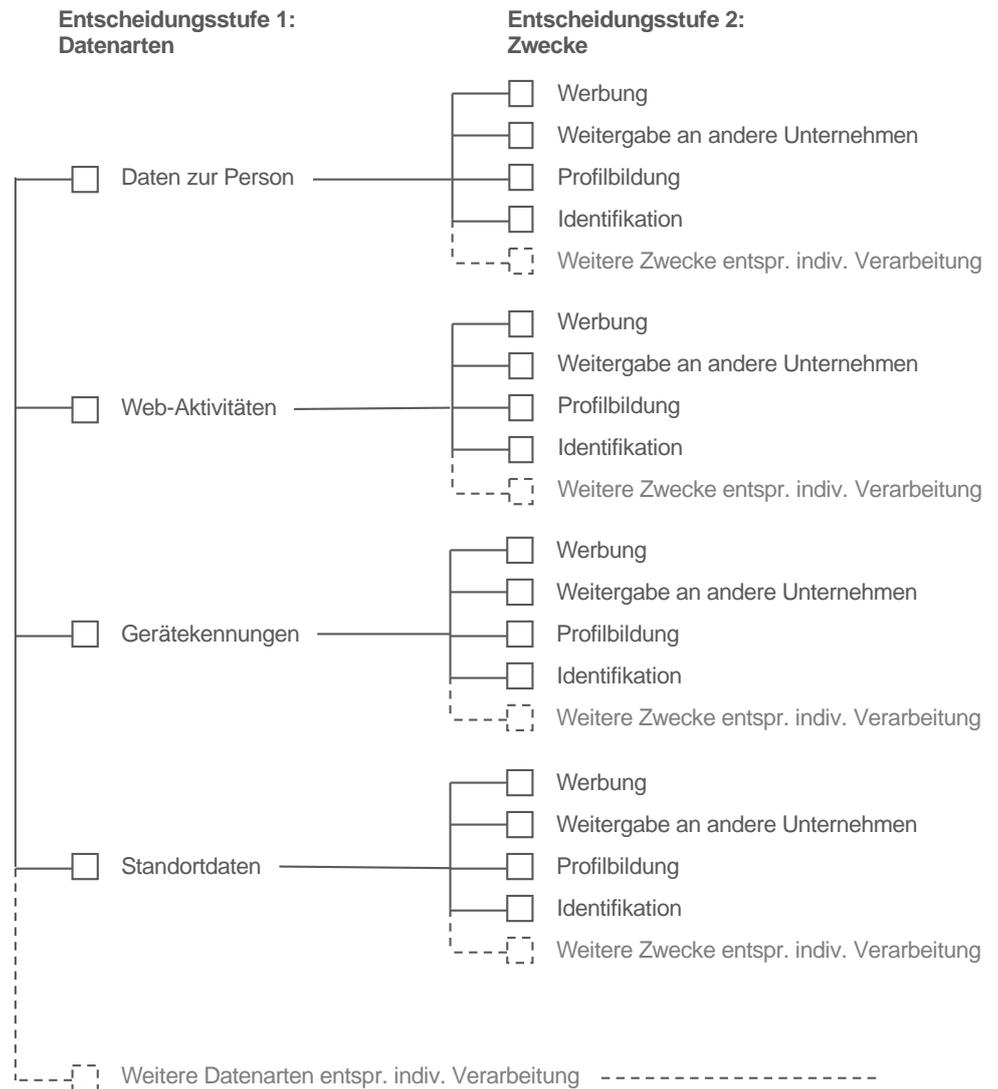


Abbildung 72: Entscheidungsbaumlogik für komplexere Datenverarbeitungen

6.2. Umsetzungsphase Einwilligung (B)

Sind alle relevanten Datenverarbeitungen definiert, die im Einwilligungsmo­dell berücksichtigt werden sollten, kann die konkrete Umsetzung erfolgen. Im ersten Schritt wird dabei die Einwilligung bei der Erstanmeldung betrachtet, die zwin­gend zum Zeitpunkt vor der tatsächlichen Verarbeitung der Daten eingeholt wer­den muss.

6.2.1. Anforderungen

6.2.1.1. Anforderung 5: *Insgesamt sollte die Einwilligung einfach bedienbar, nutzergruppenspezifisch ge­staltet und mit unterschiedlichen Endgeräten kompatibel sein.*

Auch wenn diese Anforderung offensichtlich scheint, ist eine einfache Bedien­barkeit für den Erfolg eines Einwilligungssystems unabdingbar. Dabei bedeutet einfache Bedienbarkeit auch, dass sich das System an die Anforderungen ver­schiedener Nutzergruppen anpasst. So sollte es sowohl in stationären als auch in mobilen Umgebungen funktionieren und dort benutzerfreundlich und intuitiv

umgesetzt sein. Des Weiteren sollte die Barrierefreiheit des Systems gewährleistet sein, so dass auch Nutzerinnen und Nutzer mit körperlichen Einschränkungen Zugriff auf alle Funktionen haben. Ähnliches gilt für den Schutz von Minderjährigen bei denen zusätzliche Vorgaben existieren (vgl. Abschnitt 2.1.1.7).

Die Befragung konnte zeigen, dass die getesteten, konkreten Einwilligungsmodelle allesamt gute Bewertungen im Hinblick auf deren Einfachheit erhielten (zwischen 71% und 75%, N=1.009-1.024). Auch die Übersichtlichkeit wurde insgesamt über alle Modelle hinweg eher gut bewertet (zwischen 69% und 76%, N=1.009-1.024; vgl. Abschnitt 4.1.5 und 4.1.6). Zu ähnlichen Ergebnissen kommt der Praxistest zur Einwilligung bei Miele, in dem das Modell insgesamt als eher einfach bewertet wird. So gaben 73% der befragten Kundinnen und Kunden (N=37), dass das Modell einfach oder sogar sehr einfach zu bedienen sei (vgl. Abschnitt 5.1.5). Dementsprechend sollte sich das Einwilligungs-Modell vom Umfang und der Umsetzung an den getesteten Modellen orientieren.

Neben der Bedienoberfläche können auch Hilfestellungen, die die Bedienungskomponenten erläutern und erlernbar machen, dosiert eingesetzt werden. Jedoch ersetzen diese in keinem Fall ein intuitives Bedienungskonzept und können bei inflationärem Einsatz (wie in den Theoriemodellen dargestellt) sehr ermüdend auf die Nutzerinnen und Nutzer wirken (vgl. Abschnitt 2.3.2).

6.2.1.2. Anforderung 6: Informationen zur Datenverarbeitung sollten transparent, verständlich und gestalterisch neutral in das Modell eingebunden werden. Hierbei ist die richtige Dosierung wichtig.

Aus rechtlicher Perspektive ist es erforderlich, dass die Nutzerinnen und Nutzer transparent über die Datenverarbeitungen informiert werden (vgl. Abschnitt 2.1.1.1). Hierbei ist aus verhaltenswissenschaftlicher Perspektive jedoch zu beachten, dass lange Texte von Verbraucherinnen und Verbrauchern oftmals nicht gelesen werden. So kann ein Informationsüberfluss („Information Overload“) schnell zu einem frustrierenden Nutzungserlebnis führen, bei dem Verbraucherinnen und Verbraucher das Lesen ggf. vorzeitig abbrechen (vgl. Abschnitt 2.1.2.2.1).

Des Weiteren ist es grundsätzlich aus rechtlicher Perspektive unproblematisch, Informationen hinter Verlinkungen einzubinden (jedenfalls für den ersten Link, Verschachtelungen sind unzulässig). Aus verhaltenswissenschaftlicher Sicht kann eine Verlinkung jedoch zu einer reduzierten Zugänglichkeit führen; somit besteht die Gefahr, dass sich Verbraucherinnen und Verbraucher die Informationen nicht ansehen (vgl. Abschnitt 2.1.2.2.4).

Trotz dieser möglichen Einschränkungen sind die Bedürfnisse und Erwartungen der Verbraucherinnen und Verbraucher in der Befragung eindeutig: So sprechen sich die Befragten für zusätzliche (maßvolle) Erläuterungen in Pop-Ups aus (vgl. Abschnitt 4.2.3). Dieser Befund wird auch im Praxistest bei Miele bestätigt. Dort erhält das Einwilligungsmodell, das zusätzliche Erläuterungen und Pop-Ups nutzt, eine positive Bewertung mit Blick auf die Informiertheit. So geben 76% der befragten Kundinnen und Kunden (N=37) an, dass sie sich durch das Modell informiert oder sogar sehr informiert fühlen (vgl. Abschnitt 5.1.4). Es ist hierbei jedoch anzumerken, dass in der Befragung und im Praxistest kurze, prägnante

und verständliche Informationen zu den Datenverarbeitungen eingesetzt wurden. Wie die Verbraucherinnen und Verbraucher zu längeren Texten stehen, ist unklar und sollte bei der Implementierung des Modells mitgedacht werden.

6.2.1.3. Anforderung 7: Für die einwilligungsrelevanten Aspekte muss das Modell datensparsame Voreinstellungen vorsehen.

Entscheidungssituationen können grundsätzlich so ausgestaltet sein, dass Wahloptionen von den verarbeitenden Stellen voreingestellt sind, oder, dass bewusst keine Voreinstellung gewählt ist und sich Verbraucherinnen und Verbraucher aktiv entscheiden müssen, um im Prozess weiterzukommen. Die Befragungsergebnisse ergeben ein klares Votum für Voreinstellungen von Wahleinstellungen (vgl. Abschnitt 4.2.1): Bei den paarweisen Vergleichen in der Befragung präferiert die Mehrheit der Verbraucherinnen und Verbraucher Voreinstellungen gegenüber einer Wahlentscheidung ohne Voreinstellung. Dies gilt sowohl für Voreinstellungen, bei denen die Datenverarbeitung aktiviert ist, als auch bei solchen, die „keine Datenverarbeitung“ voreinstellen.

Aus rechtlicher Perspektive sind Voreinstellungen – so lange sie die datensparsame Verarbeitung vorsehen – ebenfalls begrüßenswert auch wenn Wahleinstellungen ohne eine Voreinstellung prinzipiell ebenso rechtmäßig sind (vgl. Abschnitt 2.3.1).

Lediglich aus verhaltenswissenschaftlicher Sicht bergen Voreinstellungen ein potentielles Risiko, denn Verbraucherinnen und Verbraucher tendieren häufig dazu, in den Voreinstellungen zu verbleiben (vgl. Abschnitt 2.1.2.2.3). Werden daher datensparsame Voreinstellungen gesetzt, ist davon auszugehen, dass Personen, die wenig Datenschutzbedenken haben, tendenziell die datensparsame Voreinstellung beibehalten, auch wenn dies nicht ihrer Präferenz entspricht.

Die Ergebnisse aus dem Praxistest zur Einwilligung bei Miele, bei dem die Voreinstellungen zur Datenverarbeitung allesamt datensparsam gesetzt wurden, zeigen, dass Verbraucherinnen und Verbraucher das Modell allgemein gut bis sehr gut bewerten (84% der Befragten, N=37, vgl. Abschnitt 5.1.1). Zwar ist es dabei nicht eindeutig, ob dies auf die Differenzierung und die Voreinstellungen zurückzuführen ist, doch das Ergebnis ist ein Indiz für die Gesamtpformance des Modells, das diese Voreinstellungen beinhaltet.

6.2.1.4. Anforderung 8: Übergeordnet darf das Modell nicht vom Wesentlichen ablenken. Weiterhin ist eine manipulierende Gestaltung oder Framing der Modellinhalte zu unterlassen.

Diese übergeordnete Anforderung erscheint auf den ersten Blick offensichtlich, sollte vor dem Hintergrund der Diskussion über „deceptive designs“ jedoch nicht unterschätzt werden. Die Bestandsaufnahme und Ergebnisse aus der Literatur konnten zeigen, dass oftmals gestalterische Maßnahmen genutzt werden, um Verbraucherinnen und Verbraucher von Datenschutzaspekten abzulenken. Hier ist die verhaltenswissenschaftliche Literatur eindeutig: Verbraucherinnen und Verbraucher sollten nicht durch unnötige Texte abgelenkt werden und auch ein Framing, bei dem die Vertrauenswürdigkeit des Anbieters überbordend betont wird, kann irreführend wirken. Entsprechend ist es unabdingbar, ein neutrales

Einwilligungsmodell zu entwerfen, das die Aufmerksamkeit der Nutzerinnen und Nutzer fördert (vgl. Abschnitt 2.1.2.2.2 und 2.1.2.2.6).

Darüber hinaus sind subtile und manipulative Gestaltungsmaßnahmen zu unterlassen, die die Entscheidungen der Verbraucherinnen und Verbraucher zwischen Zustimmung und Ablehnung der Datenverarbeitung möglicherweise in eine unerwünschte Richtung beeinflussen. So sollten grafische Darstellungen nicht dahingehend genutzt werden, dass sich Verbraucherinnen und Verbraucher einer Option mehr oder weniger hingezogen fühlen, bspw. indem Schaltflächen farblich hinterlegt werden oder unterschiedliche Schriftarten eingesetzt werden. Auch ist sog. Framing zu vermeiden und die Einstellungsmöglichkeiten müssen für alle wählbaren Optionen einfach und intuitiv nutzbar sein, ohne dass Hürden den Bedienvorgang erschweren (vgl. 2.1.2.2.5).

6.2.2. Illustration der Umsetzung

Diese Anforderungen gilt es sodann in die Praxis umzusetzen:

Zunächst sollte in der Entwicklung des Modells die Nutzerfreundlichkeit mitgedacht und fortlaufend getestet werden. Auch ist es notwendig, unterschiedliche Endgeräte mitzudenken. Insbesondere Anbieter, die mobile und stationäre Umgebungen bespielen, sollten dies beim Entwerfen der Modell-Lösung berücksichtigen.

Zur übergeordneten Orientierung sind aus Usability-Sicht insgesamt sieben Anforderungen zu erfüllen, so dass das Modell verbraucherfreundlich ist (vgl. Krug, 2014).²³³

1. Das Modell und dessen Funktionen sollten **nützlich** sein, das heißt Nutzerinnen und Nutzer ziehen einen Mehrwert aus ihnen.
2. Das Modell und dessen Funktionen sollten **erlernbar** sein, das heißt Nutzerinnen und Nutzer sind in der Lage, eigenständig und einfach herauszufinden, wie diese funktionieren.
3. Das Modell und dessen Funktionen sollten **einprägsam** sein, das heißt nach einmaligem Verstehen muss die Anwendung / Funktion nicht erneut erlernt werden.
4. Das Modell und dessen Funktionen sollten **effektiv**, das heißt wirksam sein.
5. Das Modell und dessen Funktionen sollten **effizient** sein, das heißt in einem verhältnismäßig geringen (zeitlichen) Aufwand zum Ziel führen.
6. Das Modell und dessen Funktionen sollten **begehrntwert** sein, das heißt von Nutzerinnen und Nutzern als attraktiv empfunden werden.
7. Das Modell und dessen Funktionen sollten **reizvoll** sein, das heißt Nutzerinnen und Nutzer haben bei der Bedienung Freude und Spaß.

²³³ Krug, S. (2014). Don't make me think! Revisited. Web & Mobile Usability; S. 9

Aufbauend auf den in Abschnitt 6.1.2 definierten Datenverarbeitungen müssen zu diesen Datenverarbeitungen entsprechende verständliche Texte verfasst werden. Diese sollten sprachlich einfach verständlich sein und über das Wesentliche informieren. Auch hier ist eine Testung der Texte an den Nutzerinnen und Nutzern sinnvoll und sollte bei der Entscheidung über die richtige Dosierung mitgedacht werden. Aus gestalterischer Sicht ist eine Einbindung von Erläuterungen über Pop-Ups empfehlenswert. Auf diese Weise sind die erläuternden Texte verfügbar und einfach zugänglich.

Darüber hinaus sollten die einwilligungsrelevanten Aspekte eine datensparsame Voreinstellung vorsehen. Diese kann entworfen werden, in dem jeder einwilligungsrelevante Aspekt in eine zustimmende und eine ablehnende Aussage überführt wird. Vorausgewählt sollte dabei immer die ablehnende Aussage (datensparsam) sein, so dass bei Verbleiben mit der Voreinstellung keine Datenverarbeitung stattfindet. Wünschen Nutzerinnen und Nutzer eine Datenverarbeitung, können sie die Voreinstellung mit einem „Klick“ ändern.

Für die plastische Umsetzung im Fall des fiktiven „DS-Leuchtturm“-Unternehmens sieht die datensparsame Voreinstellung folgendermaßen aus (Abbildung 73):

The image shows a mock-up of a privacy settings interface for a company named 'DS-Leuchtturm AG'. The page title is 'Datenschutz-Einstellungen (1/4)'. Under the heading 'Daten zu Ihrer Person', there are two sections:

- Personalisierte Werbung**: Two radio button options are shown. The first is 'Verarbeitung meiner Daten für personalisierte Werbung zustimmen' (unchecked). The second is 'Verarbeitung meiner Daten für personalisierte Werbung nicht zustimmen' (checked).
- Weitergabe an andere Unternehmen**: Two radio button options are shown. The first is 'Weitergabe meiner Daten an andere Unternehmen zustimmen' (unchecked). The second is 'Weitergabe meiner Daten an andere Unternehmen nicht zustimmen' (checked).

At the bottom, there is a note: 'Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzerklärung](#).' and a green button labeled 'Weiter'.

Abbildung 73: Best Practice-Modell – Mock-Ups "Datensparsame Voreinstellungen"

Die Umsetzung des Pop-Ups mit Erläuterungstext sieht wie folgt aus (Abbildung 74):

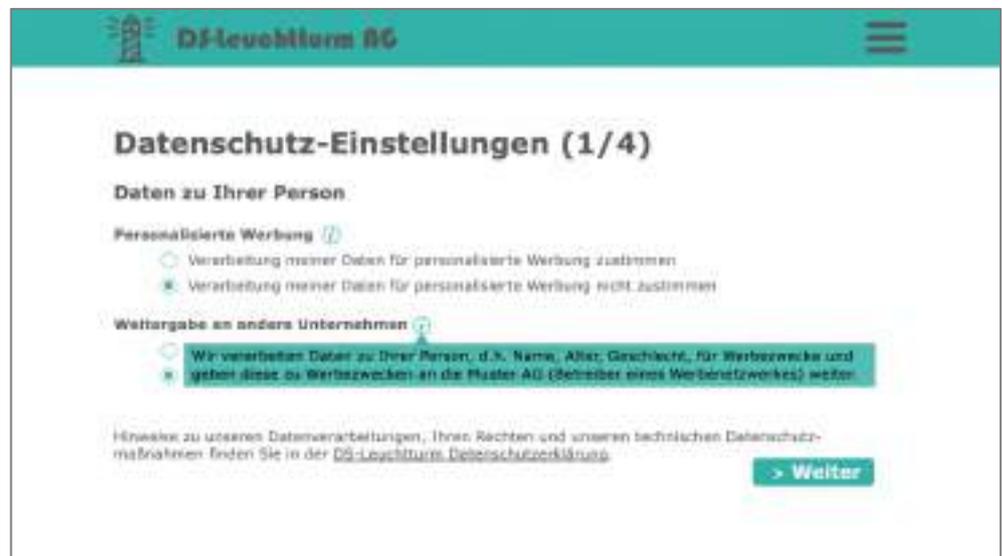


Abbildung 74: Best Practice-Modell – Mock-Ups "Erläuternde Texte in Pop-Ups"

Um eine Kompatibilität mit mobilen Endgeräten sicherzustellen, sollte die Umsetzung der Datenschutz-Einstellungen und Pop-Ups mit Erläuterungstexten angepasst werden. Abbildung 75 zeigt die Mock-Ups.



Abbildung 75: Best Practice-Modell – Mock-Ups "Datensparsame Voreinstellungen" und "Erläuternde Texte in Pop-Ups" (Mobile Endgeräte)

Bei komplexeren Systemen, bei denen eine Vielzahl von Datenarten mit Verarbeitungszwecken kombiniert werden, sollte auf der Grundlage der Entscheidungsbaumlogik (vgl. Abbildung 72) ein Zwischenschritt eingefügt werden. Die Anpassung der Einwilligungen erfolgt dann über zwei Stufen.

In der ersten Stufe sollten Nutzerinnen und Nutzer die Möglichkeit erhalten, zu entscheiden, für welche spezifischen Datenarten Datenschutz-Einstellungen vorgenommen werden sollen. Die abgefragten Datenarten sollten dabei nicht vorausgewählt sein, sondern durch entsprechende Auswahl ausgewählt werden

können. Abbildung 76 zeigt diesen Zwischenschritt. Wenn Nutzerinnen und Nutzer in der ersten Stufe entscheiden, dass sie keine Verarbeitung ihrer Daten möchten, ist die Anmeldung und somit der Einwilligungsvorgang bereits an dieser Stelle abgeschlossen.



Abbildung 76: Best Practice-Modell – Mock-Ups "Auswahl der Datenschutz-Einstellungen" in komplexeren Systemen (Stufe 1)

Stimmen sie einer Verarbeitung zu, werden dann in der zweiten Stufe nur die Verarbeitungszwecke abgefragt, die zu den vorher ausgewählten Datenarten gehören. Die grafische und inhaltliche Umsetzung in der zweiten Stufe erfolgt dabei analog zu den Datenschutz-Einstellungen im „einfachen“ Best Practice-Modell.

Wenn also Nutzerinnen und Nutzer in der ersten Stufe entscheiden, dass sie lediglich Einstellungen zu „Webaktivitäten“ und „Standortdaten“ vornehmen möchten, werden auf den Folgeseiten im Anmeldeprozess auch nur Einwilligungsentscheidungen zu „Webaktivitäten“ und „Standortdaten“ angezeigt – nicht jedoch zu „Daten zur Person“ und zu „Gerätekennungen“.

6.3. Umsetzungsphase Management der Einwilligung (C)

Neben der Einwilligung bei der Anmeldung ist es auch notwendig, die getätigten differenzierten Einwilligungen verwalten zu können und so Einwilligungen zu widerrufen oder auch später zu erteilen. Eine entsprechende Umsetzung wird im Folgenden beschrieben.

6.3.1. Anforderungen

6.3.1.1. Anforderung 9: Zur nachträglichen Verwaltung der erteilten Einwilligungen und Datenverarbeitungen sowie zur erleichterten Ausübung von Datenschutz-Nutzungsrechten sollte ein Datenschutz-Cockpit zur Verfügung gestellt werden.

Ein Datenschutz-Cockpit ist eine Nutzeroberfläche, in der Nutzerinnen und Nutzer ihre Einwilligungen einsehen können. Darüber hinaus ermöglicht das Cockpit

den Nutzerinnen und Nutzern – in Anlehnung an die Steuerung eines Flugzeuges – aktiv und autonom die Steuerung darüber zu übernehmen, welche Daten für welche Zwecke verarbeitet werden dürfen. Hierfür können im Datenschutz-Cockpit neue Einwilligungen gegeben werden oder aber alte widerrufen werden.²³⁴ Neben dem Widerruf der Einwilligungen sollten im Datenschutz-Cockpit ebenfalls die Datenverarbeitungen nach berechtigtem Interesse transparent gemacht werden und hierfür einfache Widerspruchsmöglichkeiten eingeräumt werden.

Aus rechtlicher Sicht existieren keine Einwände gegen den Einsatz von Datenschutz-Cockpits, die den Verbraucherinnen und Verbrauchern ein Einwilligungsmanagement im Nachhinein ermöglichen (vgl. Abschnitt 2.3.1). Jedoch dürfen diese die Einwilligung im Vorhinein nicht ersetzen. Überdies würden solche Cockpits es Nutzerinnen und Nutzern ermöglichen, von ihrem Widerrufsrecht effektiv und in differenzierter Art und Weise Gebrauch zu machen.

Die Befragung zeigt, dass Verbraucherinnen und Verbraucher eine solche Funktion insgesamt gut bewerten. So geben 77% der Befragten (N=2.029) an, dass aus ihrer Sicht ein Cockpit gut oder sogar sehr gut sei (vgl. Abschnitt 4.3). Und auch aus verhaltenswissenschaftlicher Sicht sind solche Cockpits insgesamt positiv zu bewerten, da sie die Wahlfreiheit der Verbraucherinnen und Verbraucher begünstigen (vgl. Abschnitt 2.3.1). Jedoch muss auch hier sichergestellt werden, dass Verbraucherinnen und Verbraucher die Funktion tatsächlich und regelmäßig nutzen.

Weitere Indizien für die Empfehlung ein Datenschutz-Cockpit einzubinden, ergeben sich aus dem zweiten Praxistest bei der Telekom. Das untersuchte Status-Quo-Modell, welches in seiner Ausgestaltung textbasiert ist und Einstellungsmöglichkeiten über Check-Boxen erlaubte, wurde insgesamt positiv bewertet. So gaben über alle Bewertungsdimensionen hinweg durchschnittlich zwei Drittel der Befragten an, dass das Modell bspw. verständlich und hilfreich sei, sowie einen Mehrwert bieten würde. Das zweite Modell, das neugestaltete Datenschutz-Cockpit mit Schiebereglern, erhielt über die Bewertungsdimensionen hinweg sogar eine noch bessere Bewertung durch die Kundinnen und Kunden.

6.3.2. Illustration der Umsetzung

Gegeben der Anforderungen können diese folgendermaßen in die Praxis umgesetzt werden:

Zuerst sollte entschieden werden, ob die Einwilligungen im Cockpit nach Datenarten oder Verarbeitungszwecken sortiert werden. Im Beispiel des „DS-Leuchtturm“ wurde – analog zur Einwilligung bei der Anmeldung – eine Sortierung nach Datenarten mit entsprechend differenzierten Unterzwecken vorgenommen. Prinzipiell ist jedoch eine Umsortierung denkbar.

²³⁴ Dabei ist das Datenschutz-Cockpit also von einem Datenschutz-Dashboard abzugrenzen, da letzteres lediglich eine Transparenzfunktion übernimmt und Nutzerinnen und Nutzern anzeigt, welche Daten verarbeitet werden, nicht jedoch Einstellungsmöglichkeiten bietet.

Die Inhalte, die im Cockpit angezeigt werden, müssen zwingend den vorgenommenen Einstellungen aus der Einwilligung bei der Anmeldung entsprechen. Haben Nutzerinnen und Nutzer dabei einer Verarbeitung zugestimmt, so muss sich diese Zustimmung auch im Cockpit wiederfinden.

Im fiktiven Beispiel des „DS-Leuchtturm“ hat der Nutzer folgenden Datenverarbeitungen zugestimmt:

- *Daten zur Person zur Weitergabe an andere Unternehmen*
- *Webaktivitäten zur Profilbildung*
- *Standortdaten für Werbezwecke und Profilbildung*

Folgende Datenverarbeitungen wurden abgelehnt:

- *Daten zur Person für persönliche Werbung*
- *Gerätekennungen zur Identifikation*

Weiterhin müssen im Cockpit – analog zur Einwilligung bei der Anmeldung – transparente Informationen zu den Datenverarbeitungen vorliegen. Wurde dabei mit einem bestimmten Symbol und Pop-Ups gearbeitet, so sollte dies auch im Cockpit der Fall sein, um den Wiedererkennungswert zu steigern und die intuitive Nutzung zu fördern. Gestalterisch gibt es bei der Umsetzung der Einstellungsmöglichkeiten Freiraum. Selbstverständlich ist auch weiterhin eine Formulierung und Anordnung der Optionen zu verwenden, die frei von Manipulation ist.

In der praktischen Umsetzung des „DS-Leuchtturm“ wurden dabei Schieberegler genutzt, wie sie oftmals in Cockpits zum Einsatz kommen (vgl. Abbildung 77 für Desktop und Abbildung 78 für mobile Endgeräte). Ein weiterer Grund für den Einsatz der Schieberegler war weiterhin das bessere Abschneiden dieses Ausgestaltung im Praxistest bei der Telekom. Wichtig ist bei der Gestaltung, dass es den Nutzerinnen und Nutzern klar sein muss, wann eine Einwilligung als erteilt anzusehen ist und wann nicht.



Abbildung 77: Best Practice-Modell – Mock-Ups "Datenschutz-Cockpit"



Abbildung 78: Best Practice-Modell – Mock-Ups "Datenschutz-Cockpit" (Mobile Endgeräte)

Zu guter Letzt ist auch beim Entwurf und der Weiterentwicklung des Cockpits eine Testung an Nutzerinnen und Nutzern hilfreich. So können Nutzerorientierung und Verständlichkeit getestet werden.

6.4. Optionale Zusatzfunktionen

Im letzten Schritt werden weitere optionale Funktionen vorgestellt, die das Best Practice-Modell ergänzen können.

6.4.1. Anforderungen

6.4.1.1. Anforderung 10: Visualisierungen wie Icons oder Piktogramme können als Hilfestellung für die Verständlichkeit der Datenverarbeitung genutzt werden.

Umgangssprachlich wird häufig konstatiert, dass ein Bild „mehr als tausend Worte“ sagt. So werden bei Datenverarbeitungen unterschiedliche Symbole in Form von Icons bzw. Piktogrammen diskutiert, die das Verständnis der Verbraucherinnen und Verbraucher fördern sollen. Die Befragungsergebnisse zeigen, dass Verbraucherinnen und Verbraucher Visualisierungen von Datenschutxtexten in Form von Piktogrammen oder Icons prinzipiell gut finden, wenn auch sie diese nicht als prioritär ansehen. So sagten 56% der Befragten (N=2.029), dass die Einbindung von Piktogrammen gut oder sogar sehr gut sei (vgl. Abschnitt 4.3). Aus rechtlicher Sicht sind Visualisierungen zulässig, wenn sie bspw. zur Verständlichkeit der Texte beitragen; sie können und dürfen Texte jedoch nicht ersetzen. Ferner können sie aus verhaltenswissenschaftlicher Sicht bei schlechter Gestaltung auch ihren Zweck verfehlen und Verbraucherinnen und Verbraucher überfordern, weil die Interpretation nicht eindeutig ist (vgl. Abschnitt 2.3.4).

Sollten Visualisierungen eingesetzt werden, sollten diese einheitlich gestaltet werden und so eine Vergleichbarkeit über unterschiedliche Dienste und Anbieter

ermöglichen. Darüber hinaus sollten die Formate vorab getestet werden, damit die Verständlichkeit für die Verbraucherinnen und Verbraucher gewährleistet ist.

6.4.1.2. Anforderung 11: Eine Erinnerungsfunktion zum Überprüfen der Datenschutzeinstellungen kann das Modell sinnvoll ergänzen.

Eine weitere Zusatzfunktion könnte eine Erinnerungsfunktion für Datenschutzeinstellungen sein. Nach einem bestimmten Zeitraum, bspw. sechs Monaten, würden Nutzerinnen und Nutzer daran erinnert, das Einwilligungsmanagementsystem zu besuchen. Somit würden sie die Einstellungen nicht vergessen und hätten Gelegenheit, ihre vorher getätigten Entscheidungen mit ihren aktuellen Präferenzen abzugleichen. (Da diese Erinnerungsfunktion eine weitere, einwilligungsrelevante Datenverarbeitung darstellt, sollte auch hier – analog zur Umsetzung im vorgestellten Best Practice-Modell – eine Einwilligung eingeholt bzw. deren Widerruf ermöglicht werden.)

Insgesamt wird die Erinnerungsfunktion für Datenschutzeinstellungen von den Teilnehmerinnen und Teilnehmern in der Befragung positiv bewertet. So gaben 51% der Befragten (N=2.029) an, dass eine solche Funktion gut oder sogar sehr gut sei. Doch auch sie stellt keine prioritäre Forderung dar (vgl. Abschnitt 4.3). Auch aus rechts- und verhaltenswissenschaftlicher Sicht spricht nichts gegen den Einsatz; Anbieter können so bei der Gestaltung ihrer Einwilligungsmanagementsysteme abwägen, ob sich eine Implementierung lohnt (vgl. Abschnitt 2.3.4).

6.4.2. Illustration der Umsetzung

Für beide und alle weiteren denkbaren Zusatzfunktionen ist es wichtig, neben rechtlichen Vorgaben den Blick der Nutzerinnen und Nutzer einzunehmen. Je mehr vorab getestet werden kann, desto besser. So kann auch vermieden werden, dass Funktionen eingeführt werden, die später nicht genutzt werden.

6.5. User Journey: Mock-Ups der Umsetzung

Die folgenden Abbildungen zeigen die Mock-Ups des Best Practice-Modells für das fiktive Unternehmen „DS-Leuchtturm AG“.

Zu Beginn findet sich die Anmeldeseite, auf der Nutzerinnen und Nutzer Daten zu ihrer Person eintragen. Hierbei ist darauf zu achten, dass der Grundsatz der Datenminimierung einzuhalten ist. Im dargestellten Szenario der DS-Leuchtturm AG gehen wir davon aus, dass die abgefragten Daten tatsächlich für die Vertragserfüllung notwendig sind. Hiernach können die Nutzerinnen und Nutzer ihre Datenschutzeinstellungen zu den einwilligungsrelevanten Datenverarbeitungen vornehmen. Dazu sind vier Seiten zur (i) Verarbeitung der Daten zur Person, (ii) Web-Aktivitäten, (iii) Gerätedaten und (iv) Standortdaten vorgesehen, auf denen einzelne Verarbeitungszwecke ausgewählt werden können. Zusätzliche Erläuterungen werden über Pop-Ups erreicht.

Am Ende des Anmeldeprozess werden die gewählten Einstellungen außerdem im Datenschutz-Cockpit zusammengefasst und können hier weiter angepasst werden.



The image shows a registration form for 'DS-Leuchtturm AG'. The header is teal with the company logo and name. The main heading is 'Anmeldung: Daten zu Ihrer Person'. The form includes fields for gender (Frau, Herr, Keine Angabe), first name, last name, email, and birth date (split into Tag, Monat, Jahr). There is a password field. A link to the privacy policy is provided, and a 'Weiter' button is at the bottom right.

Anmeldung: Daten zu Ihrer Person

Anrede
 Frau Herr Keine Angabe

Vorname Nachname

E-Mail

Geburtsdatum
Tag Monat Jahr

Passwort

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren betrieblichen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzerklärung](#).

[> Weiter](#)



The image shows the same registration form as above, but with example data filled in. The gender is 'Herr', first name is 'Max', last name is 'Mustermann', email is 'max@mustermann.de', and birth date is '22 März 1981'. The password field is masked with dots. The 'Weiter' button is still present.

Anmeldung: Daten zu Ihrer Person

Anrede
 Frau Herr Keine Angabe

Vorname Nachname

E-Mail

Geburtsdatum
Tag Monat Jahr

Passwort

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren betrieblichen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzerklärung](#).

[> Weiter](#)

DF-Leuchtturm AG

Datenschutz-Einstellungen

Neben den Daten, die für die Vertragserfüllung notwendig sind, können Sie zusätzlich entscheiden, ob Sie weiteren Datenverarbeitungen zustimmen möchten.

Ich möchte zusätzliche Datenschutz-Einstellungen vornehmen zu

- Daten zu meiner Person
- Web-Aktivitäten
- Gerätekennungen
- Standortdaten

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzerklärung](#).

> Anmelden

DF-Leuchtturm AG

Datenschutz-Einstellungen (1/4)

Daten zu Ihrer Person

Personalisierte Werbung ⓘ

- Verarbeitung meiner Daten für personalisierte Werbung zustimmen
- Verarbeitung meiner Daten für personalisierte Werbung nicht zustimmen

Weitergabe an andere Unternehmen ⓘ

- Weitergeben meiner Daten an andere Unternehmen zustimmen
- Weitergeben meiner Daten an andere Unternehmen nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzerklärung](#).

> Weiter

DF-Leuchtturm AG

Datenschutz-Einstellungen (1/4)

Daten zu Ihrer Person

Personalisierte Werbung ⓘ

- Wir verarbeiten Daten zu Ihrer Person, d.h. Name, Alter, Geschlecht, für personalisierte Werbung. Diese Werbung wird auf Grundlage Ihrer Daten und des durch uns erhobenen Profils auf Sie abgestimmt.
- Werbung. Diese Werbung wird auf Grundlage Ihrer Daten und des durch uns erhobenen Profils auf Sie abgestimmt.

Weitergabe an andere Unternehmen ⓘ

- Weitergeben meiner Daten an andere Unternehmen zustimmen
- Weitergeben meiner Daten an andere Unternehmen nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzerklärung](#).

> Weiter

DF-Leuchtturm AG

Datenschutz-Einstellungen (1/4)

Daten zu Ihrer Person

Personalisierte Werbung

- Verarbeitung meiner Daten für personalisierte Werbung zustimmen
- Verarbeitung meiner Daten für personalisierte Werbung nicht zustimmen

Weitergabe an andere Unternehmen

- Wir verarbeiten Daten zu Ihrer Person, d.h. Name, Alias, Geschlecht, für Werbezwecke und geben diese zu Werbezwecken an die Muster AG (Betreiber eines Werbenetzwerkes) weiter.
- Weitergabe meiner Daten an andere Unternehmen nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzklärung](#).

[> Weiter](#)

DF-Leuchtturm AG

Datenschutz-Einstellungen (1/4)

Daten zu Ihrer Person

Personalisierte Werbung

- Verarbeitung meiner Daten für personalisierte Werbung zustimmen
- Verarbeitung meiner Daten für personalisierte Werbung nicht zustimmen

Weitergabe an andere Unternehmen

- Weitergaben meiner Daten an andere Unternehmen zustimmen
- Weitergaben meiner Daten an andere Unternehmen nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzklärung](#).

[> Weiter](#)

DF-Leuchtturm AG

Datenschutz-Einstellungen (2/4)

Web-Aktivitäten

Web-Aktivitäten zur Profilbildung

- Speicherung meiner Web-Aktivitäten in meinem Konto zustimmen
- Speicherung meiner Web-Aktivitäten in meinem Konto nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzklärung](#).

[> Weiter](#)

DF-Leuchtturm AG

Datenschutz-Einstellungen (2/4)

Web-Aktivitäten

Web-Aktivitäten zur Profilbildung [?](#)

Mit dieser Einstellung werden Ihre Aktivitäten auf unseren Webseiten in Ihrem Konto gespeichert. Dazu zählen Suchanfragen und verknüpfte Informationen wie Ihr Standort. Außerdem werden Ihre Aktivitäten auf den Webseiten der Musterfrau GmbH gespeichert, die unsere Dienste verwendet (Verwendung des Like-Buttons). Diese Informationen werden von uns verwendet, um ein möglichst umfassendes Profil von Ihnen zu erstellen und somit unsere Dienste zu personalisieren.

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DF-Leuchtturm Datenschutz-Erklärung](#).

[> Weiter](#)

DF-Leuchtturm AG

Datenschutz-Einstellungen (2/4)

Web-Aktivitäten

Web-Aktivitäten zur Profilbildung [?](#)

Speicherung meiner Web-Aktivitäten in meinem Konto zustimmen

Speicherung meiner Web-Aktivitäten in meinem Konto nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DF-Leuchtturm Datenschutz-Erklärung](#).

[> Weiter](#)

DF-Heubühnen AG

Datenschutz-Einstellungen (3/4)

Gerätekennungen

Gerätekennungen zur Identifikation

- Speicherung meiner Gerätekennung zur Identifikation zustimmen
- Speicherung meiner Gerätekennung zur Identifikation nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Verstärkung-Datenschutzerklärung](#).

> Weiter

DF-Heubühnen AG

Datenschutz-Einstellungen (3/4)

Gerätekennungen

Gerätekennungen zur Identifikation

- Bei dieser Einstellung wird Ihre persönliche Gerätekennung in Ihrem Konto gespeichert. Diese Gerätekennung gibt es nur einmal und sie kann nur Ihnen zugeordnet werden. Somit ist es bei der wiederholten Nutzung unserer Webseiten und Apps möglich, Sie eindeutig wiederzuerkennen und Ihre Aktivitäten auf Ihr Gerät zurückzuführen. Dadurch können wir unsere Angebote genauer an Sie anpassen und Werbung anbieten.**
- Speicherung meiner Gerätekennung zur Identifikation nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Verstärkung-Datenschutzerklärung](#).

> Weiter

DF-Heubühnen AG

Datenschutz-Einstellungen (4/4)

Standortdaten

Standortdaten für Werbezwecke und Profilbildung

- Nutzung meiner Standortdaten zustimmen
- Nutzung meiner Standortdaten nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Verstärkung-Datenschutzerklärung](#).

> Anmelden

DF-Leuchtturm AG

Datenschutz-Einstellungen (4/4)

Standortdaten

Standortdaten für Werbezwecke und Profilbildung ⓘ

- Wir verarbeiten Ihre Standortdaten für kommerzielle Zwecke (Werbung). Ihre Standortdaten werden zu den gleichen Zwecken an die Muster-Karten AG weitergegeben und von dieser verarbeitet. Hierbei wird eine private Karte mit Orten, die Sie mit Ihren angemeldeten Geräten besuchen, erstellt, selbst wenn Sie gerade keines unserer Produkte nutzen.**

Hinweise
 Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm-Datenschutzerklärung](#).

[> Anmelden](#)

DF-Leuchtturm AG

Datenschutz-Einstellungen (4/4)

Standortdaten

Standortdaten für Werbezwecke und Profilbildung ⓘ

- Nutzung meiner Standortdaten zustimmen
- Nutzung meiner Standortdaten nicht zustimmen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm-Datenschutzerklärung](#).

[> Anmelden](#)

DF-Leuchtturm AG

Sie haben sich erfolgreich angemeldet!

Wenn Sie Ihre Datenschutz-Einstellungen im Überblick ansehen und anpassen wollen, besuchen Sie das **Datenschutz-Cockpit**.

[> Zum Datenschutz-Cockpit](#)

Sie können das **Datenschutz-Cockpit** auch zu späteren Zeitpunkten nutzen. Hierfür rufen Sie es bitte über das Menü auf.

DS-Leuchtturm 86
☰

Ihre persönlichen Datenschutz-Einstellungen

DS-Leuchtturm Datenschutz-Cockpit

<p>Ich stimme der Nutzung der Daten zu meiner Person für folgende Zwecke zu</p> <ul style="list-style-type: none"> <input type="checkbox"/> Personalisierte Werbung ? <input checked="" type="checkbox"/> Weitergabe an andere Unternehmen ? <p>Ich stimme der Speicherung meiner Web-Aktivitäten für folgende Zwecke zu</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Profilbildung ? 	<p>Ich stimme der Speicherung meiner Gerätebelegungen für folgende Zwecke zu</p> <ul style="list-style-type: none"> <input type="checkbox"/> Identifikation ? <p>Ich stimme der Nutzung meiner Standortdaten für folgende Zwecke zu</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Werbezwecke und Profilbildung ?
--	--

Weitere notwendige Datenverarbeitungen
 Überdies verarbeiten wir gemäß DS-GVO Art. 6 Abs. 1 lit. b. Ihre **Namen, Geschlecht, E-Mail und Geburtsdatum** zur Vertragserfüllung. Dieser Verarbeitung können Sie widersprechen. ➤ Widersprechen

Hinweise zu unseren Datenverarbeitungen, Ihren Rechten und unseren technischen Datenschutzmaßnahmen finden Sie in der [DS-Leuchtturm Datenschutzerklärung](#).

7. Literatur

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wang, Y. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3), 44.
- Anderson, B., Vance, A., Kirwan, B., Eargle, D. & Howard, S. (2014). Users aren't (necessarily) lazy: Using NeuroIS to explain habituation to security warnings. *Thirty Fifth International Conference on Information Systems*. Auckland, 2014.
- Arrow, K. J. (1950). A difficulty in the concept of social welfare. *Journal of Political Economy*, 58(4), 328-346.
- Bach, I. (2019). Neue Richtlinien zum Verbrauchsgüterkauf und zu Verbraucher-
verträgen über digitale Inhalte. *Neue Juristische Wochenschrift*, 1705-1711.
- Banerjee, A. V. (1992). A simple model of herd behavior. *The Quarterly Journal of Economics*, 107(3), 797-817.
- Bogenstahl, C. (2019). Dark Patterns – Mechanismen (be)trügerischen Internet-
designs. Büro für Technikfolgenabschätzung beim Deutschen Bundestag. Themenkurzprofil Nr. 30.
- Brink, S. & Wolf, H. A. (2020). Beck'sche Online Kommentare Datenschutzrecht. München: C.H. Beck.
- Buchner, B. (2018). Die Einwilligung in Werbung. *Wettbewerb in Recht und Praxis*, 1283-1289.
- Buchner, B. & Kühling, J. (2017). Die Einwilligung in der Datenschutzordnung 2018. *Datenschutz und Datensicherheit*, 544-548.
- Datenethikkommission. (2019). Gutachten der Datenethikkommission. Abgerufen von https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=D320786A39EF7EA4BCD184251FE7831A.1_cid364?_blob=publication-File&v=6 (15.03.2020).
- Datenschutzbeauftragter Info (13.06.2018). Die Verschlimmbesserung der Einwilligung nach der DSGVO. Abgerufen von <https://www.datenschutzbeauftragter-info.de/die-verschlimmbesserung-der-einwilligung-nach-dsgvo/> (15.03.2020).
- Demehl, S. & Hullen, N. (2013). Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa?. *Zeitschrift für Datenschutzrecht*, 147-153.
- Der Hessische Beauftragte für Datenschutz und Informationssicherheit. Häufig gestellte Frage – HGF. Abgerufen von <https://datenschutz.hessen.de/infothek/h%C3%A4ufig-gestellte-fragen-hgf> (05.05.2020).
- Dregelies, M. (2017). Wohin laufen meine Daten?. *Verbraucher und Recht*, 256-262.

- Drews, S. (2019). Kritische Betrachtung der DSK-Orientierungshilfe zur Direktwerbung. *Zeitschrift für Datenschutzrecht*, 296-301.
- Drozd, O. & Kirrane, S. (o. D.) Consent Comprehension Made Easy Demo. PET Symposium.
- DSK (2019). Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien. Abgerufen von https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf (05.05.2020).
- Duncan, J. (1984). Selective attention and the organization of visual information. *Journal of Experimental Psychology: General*, 113(4), 501.
- EDSA (2019). Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DS-GVO, insbesondere in Bezug auf die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden. Angenommen am 12. März 2019. Abgerufen von https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_de.pdf (05.05.2020).
- European Data Protection Board (EDPB) (bzw. EDSA), Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020. Abgerufen von https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (5.6.2020)
- Ehmann, E. & Selmayr, M. (2018). *Datenschutz-Grundverordnung: DS-GVO*. 2. Auflage. München: C.H. Beck.
- Engler, M. (2018). Das überschätzte Kopplungsverbot. *Zeitschrift für Datenschutzrecht*, 55-62.
- Eppler, M. J. & Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. *The Information Society*, 20(5), 325-344.
- Erd, R. (2011). Datenschutzrechtliche Probleme sozialer Netzwerke. *Neue Zeitschrift für Verwaltungsrecht*, 19-22.
- Ernst, S. (2017). Die Einwilligung nach der Datenschutzgrundverordnung. *Zeitschrift für Datenschutzrecht*, 110-114.
- EU-Kommission (2015). ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation. Final report, 2015. Abgerufen von <https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data> (06.05.2020).
- Fetzer, K.-H., Büscher, W. & Oberfell E. I. (2016). *Lauterkeitsrecht: UWG*. 3. Auflage. München: C.H. Beck.
- Figl, K. (2010). ISONORM 9241/10 und Isometrics: Usability-Fragebögen im Vergleich. Kain, Saskia (Eds.), 143-152.
- Forbruker Radet. (2018). Deceived by design. Abgerufen von <https://www.forbrukerradet.no/undersokelse/nundersokelsekategori/deceived-by-design/> (22.08.2019).

- Forgó, N., Helfrich, M. & Schneider, J. (2019). Rechtshandbuch Betrieblicher Datenschutz. 3. Auflage. München: C.H. Beck.
- Friedman, B., Lin, P. & Miller, J. K. (2005). Informed consent by design. *Security and Usability*, 2001, 503-530.
- Galetzka, C. (2019). Web-Analytics/Retargeting und automatisierte Einzelfallentscheidungen. DSRI-Tagungsband, 45-59.
- Gassner, U. (2015). MedTech meets M-Health. *Medizin Produkte Recht*, 73-82.
- Gausling, F. (2019). Künstliche Intelligenz im digitalen Marketing. *Zeitschrift für Datenschutzrecht*, 335-341.
- Gerl, A. & Prey, F. (2018). LPL Personal Privacy Policy User Interface: Design and Evaluation. *Mensch und Computer 2018-Workshopband*.
- Golland, A. (2018). Das Kopplungsverbot in der Datenschutz-Grundverordnung. *Multimedia und Recht*, 130-35.
- Hacker, P. (2019). Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht. *Zeitschrift für die gesamte Privatrechtswissenschaft*, 148-197.
- Härtig, N. (2016). *Datenschutz-Grundverordnung*. Berlin: Verlag Dr. Otto Schmidt.
- Härtig, N. (2016). Digital Goods und Datenschutz – Daten Sparen oder monetarisieren?. *Computer & Recht*, 735-740.
- Härtig, N. (2017). Kopplungsverbot nach der DSGVO. *IT_Rechtsberater*, 42-44.
- Horn, N., Riechert, A. & Müller, C. (2017). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. *Stiftung Datenschutz*. Abgerufen von https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_broschuere_20170611_01.pdf (20.08.19).
- IAPP (International Association of Privacy Professionals). (2017). White Paper – The UX Guide to Getting Consent. Abgerufen von <https://iapp.org/resources/article/the-ux-guide-to-getting-consent/> (24.07.2019).
- Joachim, K. (2017). Besonders schutzbedürftige Personengruppen. *Zeitschrift für Datenschutzrecht*, 414-418.
- Kahneman, D., Knetsch, J. L. & Thaler, R. H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. *Journal of Economic Perspectives*, 5(1), 193-206.
- Kamenica, E. (2012). Behavioral economics and psychology of incentives. *Annual Review of Economics*, 4(1), 427-452.
- Kettner, S.E., Thorun, C. & Vetter, M. (2018). Wege zur besseren Informiertheit: Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz. Abgerufen von https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf (19.07.2019).

- Körber, T. (2016). „Ist Wissen Marktmacht?“ Überlegungen zum Verhältnis Datenschutz, „Datenmacht“ und Kartellrecht – Teil 2. *Neue Zeitschrift für Kartellrecht*, 348-356.
- Kroh, N. (2016). Abschied vom Schriftformgebot der Einwilligung. *Zeitschrift für Datenschutz*, 368-373.
- Kroh, N. & Müller-Peltzer, P. (2017). Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung. *Zeitschrift für Datenschutzrecht*, 551-556.
- Kühling, J. & Buchner, B. (2018). *DS-GVO BDSG Kommentar*. 2. Auflage München: C.H. Beck.
- Kühnl, C., Rohrer, K. & Schneider, N. (2018) Ein europäischer Gesundheitsdatenschutz. *Datenschutz und Datensicherheit*, 735-740.
- Langer, E. J. (1975). The illusion of control. *Journal of Personality and Social Psychology*, 32(2), 311.
- Laugwitz, B., Schubert, U., Ilmberger, W., Tamm, N., Held, T., & Schrepp, M. (2009). Subjektive Benutzerzufriedenheit quantitativ erfassen: Erfahrungen mit dem User Experience Questionnaire UEQ. *Tagungsband UP09*.
- Lavie, N., Hirst, A., De Fockert, J. W., & Viding, E. (2004). Load theory of selective attention and cognitive control. *Journal of Experimental Psychology: General*, 133(3), 339.
- Maguire, M. (2001). Methods to support human-centred design. *International Journal of Human-Computer Studies*, 55(4), 587-634.
- McKenzie, C. R., Liersch, M. J., & Finkelstein, S. R. (2006). Recommendations implicit in policy defaults. *Psychological Science*, 17(5), 414-420.
- Metzger, A. (2016). Dienst gegen Daten: ein synallagmatischer Vertrag. *Archiv für die civilistische Praxis*, 817-864.
- Metzger, A. (2019). Digitale Mobilität – Verträge über Nutzerdaten. *Gewerblicher Rechtsschutz und Urheberrecht*, 129-136.
- Möhrke-Sobolewski, C. & Klas, B. (2016). Zur Gestaltung des Minderjährigendatenschutzes in digitalen Informationsdiensten. *Kommunikation & Recht*, 373-378.
- Nord, J. & Menzel, M. (2010). „Datenschutzerklärungen“ – misslungene Erlaubnisklausen zur Datennutzung. *Neue Juristische Wochenschrift*, 3756-3758.
- Ortner, R. & Daubenbüchel, F. (2016) *Medizinprodukte 4.0 – Haftung, Datenschutz, IT-Sicherheit*. Neue Juristische Wochenschrift, 2918-2924.
- Otto, D. & Rüdlin, M. (2017). Standardisierung von Patienteneinwilligungen im Krankenhaus. *Zeitschrift für Datenschutzrecht*, 519-524.
- Paal, B. P. & Pauly, D. A. (2018). *Datenschutz-Grundverordnung Bundesdatenschutzgesetz*. 2. Auflage. München: C.H. Beck.
- Plaut, V. C., & Bartlett, R. P. (2012). Blind consent? A social psychological investigation of non-readership of click-through agreements. *Law and Human Behavior*, 36(4), 293-311.

- Plath, K.-U. (2018). Kommentar zur DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG. 3. Auflage. Berlin: Verlag Dr. Otto Schmidt.
- Rauder, C. (2017). Gemeinsamkeiten von US Children Online Privacy Protection Act (COPPA) und DS-GVO. *Multimedia und Recht*, 15-19.
- Rauer, N. & Ettig, D. (2018). Rechtskonformer Einsatz von Cookies. *Zeitschrift für Datenschutzrecht*, 255-258.
- Riechert, A. (10.01.2017). Rechtliche Stellungnahme zur ePrivacy-Verordnung. Abgerufen von https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Ab-schluss_Studie_30032017/stiftungdatenschutz_rechtliche_Stellungnahme_e-Privacy_Richtlinie_final_01.pdf (05.05.2020)
- Säcker, F. J., Rixecker, R., Oetker, H. & Limperg, B. (2019). Münchner Kommentar zum Bürgerlichen Gesetzbuch. 8. Auflage. München: C.H. Beck.
- Sattler, A. (2017). Personenbezogene Daten als Leistungsgegenstand. *Juristen Zeitung*, 1036-1046.
- Scalable Policy-aware linked data architecture for privacy, transparency and compliance (SPECIAL). (2018). Resources. Abgerufen von <https://www.special-privacy.eu/platform> (20.08.2019).
- Schantz, P. (2016). Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht. *Neue Juristische Wochenschrift*, 1841-1847.
- Schantz, P. & Wolf, H. A. (2017). Das neue Datenschutzrecht. 1. Auflage. München: C.H.Beck
- Scheibehenne, B., Greifeneder, R., & Todd, P. M. (2010). Can there ever be too many options? A meta-analytic review of choice overload. *Journal of Consumer Research*, 37(3), 409-425.
- Schirmbacher, M. (2016). Onlinemarketing nach der DS-GVO – ein Annährungsversuch. *IT-Rechtsberater*, 274-280.
- Schneider, C., Weinmann, M., & vom Brocke, J. (2017). Digital Nudging–Guiding Choices by Using Interface Design. Schneider, C., Weinmann, M., and vom Brocke, J.(2018). Digital Nudging–Guiding Choices by Using Interface Design, *Communications of the ACM*, 61(7), 67-73.
- Schomberg, S., Barev, T. J., Janson, B. & Hupfeld, F. (2019). Ansatz zur Umsetzung von Datenschutz nach der DSGVO m Arbeitsumfeld: Datenschutz durch Nudging. *Datenschutz und Datensicherheit*, 774-780.
- Simitis, S., Hornung, G. & Spiekermann, I. (2019). *Datenschutzrecht*. Baden-Baden: Nomos.
- Specht-Riemenschneider, L. & Mantz, R. (2019). *Handbuch Europäisches und deutsches Datenschutzrecht*. 1. Auflage. München: C.H. Beck.
- Spindler, G. & Schuster, F. (2019). *Recht der elektronischen Medien*. 4. Auflage. München: C.H. Beck.
- Spindler, G., Sein, K. (2019). Die Richtlinie über Verträge über digitale Inhalte. *Multimedia und Recht*, 488-493.

- Spindler, G. (2016). Die neue EU Datenschutz-Grundverordnung. Der Betrieb, 937-947.
- Sydow, G. (2018). Europäische Datenschutzgrundverordnung. 2. Auflage. Baden-Baden: Nomos.
- Thompson, R. F., & Spencer, W. A. (1966). Habituation: a model phenomenon for the study of neuronal substrates of behavior. *Psychological Review*, 73(1), 16–43.
- Tinnefeld, M.-T. & Conrad, I. (2018). Die selbstbestimmte Einwilligung im europäischen Recht. *Zeitschrift für Datenschutzrecht*, 391-398.
- Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, 211(4481), 453-458.
- Ulbricht, M. R. & Pallas, F. (2018). Einwilligungsmangement für das Internet der Dinge. Abschlussbericht. Abgerufen von http://emidd.de/static/material/emidd/Schlussbericht_EMIDD_mitZusammenfassung_ohneZahlen.pdf (20.08.2019).
- Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un) informed Consent: Studying GDPR Consent Notices in the Field. *arXiv preprint arXiv:1909.02638*.
- Veil, W. (2015). DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip. *Zeitschrift für Datenschutzrecht*, 347-353.
- Veil, W. (2018). Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis. *Neue Juristische Wochenschrift*, 3337-3344.
- vzbv (2020). Personal Information Management Systems (PIMS). Chancen, Risiken und Anforderungen. Abgerufen von https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (09.04.2020).
- Wendehorst, C. & von Westphalen, F. (2016). Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht. *Neue Juristische Wochenschrift*, 3745-3750.
- Weichert, T. (2019). Praktische Anwendungsprobleme im Gesundheitsdatenschutz. *Medizinrecht*, 622-625.
- Werry, S. & Knoblich, S. (2017). Die neue europäische Datenschutz-Grundverordnung – Inhalte und akuter Handlungsbedarf für Pharma- und Medizinproduktunternehmer. *Medizin Produkte Recht*, 1-12.
- Wiebe, A., Helmschrot, C. (2019). Untersuchung der Umsetzung der Datenschutz-Grundverordnung (DSGVO) durch Online-Dienste. Studie im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz.
- Winter, D., Schrepp, M., & Thomaschewski, J. (2015). Faktoren der User Experience-Systematische Übersicht über produktrelevante UX-Qualitätsaspekte. *Mensch und Computer 2015 – Usability Professionals*.
- Wolf, A. (2018). Die Fernbehandlung nach dem 121. Deutschen Ärztetag im Lichte der europäischen Datenschutzgrundverordnung. *Gesundheit und Pflege*, 129-132.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems*, 26(3), 135-174.

Gesetzestexte

Richtlinie (EG) Nr. 2002/58 des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (e-Privacy-RL), in: Amtsblatt Nr. L 201 vom 31.07.2002, i.d. zuletzt geänderten Fassung v. 19. Dezember 2009, S. 37–47.

Richtlinie (EG) Nr. 95/46 des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-RL), in: Amtsblatt Nr. L 281 vom 23.11.1995, S. 31–50.

Richtlinie (EG) Nr. 2009/136 des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, in: Amtsblatt Nr. L 337, vom 18.12.2009, S. 11 ff.

Richtlinie (EU) Nr. 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DI-RL), in: Amtsblatt Nr. L 136, S. 1.

Richtlinie (EWG) Nr. 93/13 des Rates vom 5. April 1993 über missbräuchliche Klauseln in Verbraucherverträgen, in: Amtsblatt Nr. L 95 vom 21.04.1993, S. 29.

Verordnung (EU) Nr. 2016/679: Verordnung 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 (DSGVO), in: Amtsblatt Nr. L 119 vom 04.05.2016, S. 1–88.

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 Richtlinie 2002/58/EG (e-Privacy-VO-E), COM/2017/010 final, 2017/03 (COD). Abgerufen von:

<https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52017PC0010> (05.05.2020).

8. Anhang

Anhang A: Befragungskonzept Verbraucherbefragung

A.1. Mock-Ups Modell v1 (globale Einwilligung)

The image shows a browser window with the URL <https://www.technismart.de/anmeldung>. The page title is "TechniSmart: Anmeldung". The main heading is "Konto erstellen". The form includes the following fields:

- Fr Name:
- E-Mail:
- Passwort:
- Passwort erneut eingeben:
- Fr Geburtstag: Tag Monat Jahr
- Fr Geschlecht: Geschlecht

Buttons: "Abbrechen" and "Konto erstellen".

Text at the bottom: "Mit Ihrer Anmeldung erklären Sie sich mit unseren [Datenschutzbestimmungen](#) einverstanden."

Callout 1 (left): "Zuerst sieht der Nutzer die Anmeldeseite."

Callout 2 (right): "Unten befindet sich ein Link, der ihn auf die Seite der Datenschutzbestimmungen führt. Er kann den Link anklicken, muss es aber nicht."

TechniSmart: Anmeldung x TechniSmart: Datenschutz x

← → C https://www.technismart.de/datenschutz

TechniSmart
Datenschutz

Wenn er den Link klickt, sieht er die Datenschutzbestimmungen.

1. Welche Daten verarbeitet TechniSmart?
TechniSmart bietet Ihnen verschiedene Services, die Sie auch auf unterschiedliche Weise nutzen können. Je nachdem, ob Sie online, telefonisch, persönlich oder auf andere Weise mit uns in Kontakt treten und welche Services Sie nutzen, fallen dabei verschiedene Daten aus unterschiedlichen Quellen an. Viele der von uns verarbeiteten Daten teilen Sie uns selbst mit, wenn Sie unsere Services nutzen oder mit uns in Kontakt treten, beispielsweise wenn Sie sich registrieren und dafür Ihren Namen oder Ihre E-Mail-Adresse oder Ihre Anschrift angeben. Wir erhalten aber auch technische Geräte- und Zugriffsdaten, die bei Ihrer Interaktion mit unseren Services automatisch von uns erfasst werden. Dabei kann es sich beispielsweise um Informationen darüber handeln, welches Gerät Sie nutzen. Weitere Daten erheben wir durch eigene Datenanalysen (z.B. im Rahmen von Marktforschungsstudien und durch Auswertung von Kunden).

2. Wozu verwendet TechniSmart meine Daten?
TechniSmart verarbeitet Ihre Daten unter Einhaltung aller anwendbaren Datenschutzgesetze. Dabei beachten wir selbstverständlich die Grundsätze des Datenschutzes für die Verarbeitung personenbezogener Daten. Ihre Daten verarbeiten wir daher grundsätzlich nur zu den Ihnen in dieser Datenschutzerklärung erläuterten oder bei der Erhebung der Daten mitgeteilten Zwecken. Diese sind in erster Linie die Einkaufsabwicklung und die Bereitstellung, Personalisierung und Weiterentwicklung sowie die Sicherheit unserer Services. Daneben verwenden wir Ihre Daten im Rahmen des strengen deutschen und europäischen Datenschutzrechts aber auch für weitere Zwecke, etwa Produktentwicklung, wissenschaftliche Forschung (insbesondere in den Bereichen maschinelles Lernen, künstliche Intelligenz und Deep Learning) und Marktforschung, für die Optimierung von Geschäftsprozessen, die bedarfsgerechte Gestaltung unserer Services sowie für personalisierte Werbung.

3. Personalisierte Services
Die Entwicklung und Bereitstellung von personalisierten Funktionalitäten und Services für Sie hat bei uns oberste Priorität. Wir bieten Ihnen unabhängig von Ort, Zeit und verwendeten Geräten ein individuelles Shopping-Erlebnis und ein auf Ihre individuellen Interessen zugeschnittenes Angebot. Die Verarbeitung Ihrer Daten zur Personalisierung unserer Services ist bei TechniSmart daher fester Leistungsbestandteil.

TechniSmart: Anmeldung x

← → C https://www.technismart.de/anmeldung

Konto erstellen

TechniSmart

Ihr Name
Stefan Mustermann

E-Mail
stefan@mustermann.de

Passwort
••••••••

Passwort erneut eingeben
••••••••

Ihr Geburtstag
22 August 1981

Ihr Geschlecht
männlich

Abbrechen **Konto erstellen**

Nach dem Eintragen der Daten, kann der Nutzer auf „Konto erstellen“ klicken und der Anmeldevorgang ist abgeschlossen.

Mit Ihrer Anmeldung erklären Sie sich mit unseren [Datenschutzbestimmungen](#) einverstanden.

A.2. Mock-Ups Model v2 (erzwungene Einwilligung)

TechniSmart: Anmeldung x
 https://www.technismart.de/anmeldung

Konto erstellen

Techni Smart

Zuerst sieht der Nutzer die Anmeldeseite.

Ihr Name

 E-Mail

 Passwort

 Passwort erneut eingeben

 Ihr Geburtstag
 Tag Monat Jahr
 Ihr Geschlecht
 Geschlecht

Ich bin damit einverstanden, dass meine Daten für Werbezwecke verarbeitet und auch an andere Unternehmen weitergegeben werden. Diese Einwilligung kann jederzeit auf www.technismart.de/abmelden widerrufen werden.

Abbrechen Konto erstellen

TechniSmart: Anmeldung x
 https://www.technismart.de/anmeldung

Konto erstellen

Techni Smart

Die Einwilligung für Werbezwecke hat er nicht ausgewählt.

Ihr Name

 E-Mail

 Passwort

 Passwort erneut eingeben

 Ihr Geburtstag
 22 August 1981
 Ihr Geschlecht
 männlich

Ich bin damit einverstanden, dass meine Daten für Werbezwecke verarbeitet und auch an andere Unternehmen weitergegeben werden. Diese Einwilligung kann jederzeit auf www.technismart.de/abmelden widerrufen werden.

Nachdem er seine Daten eingetragen hat, möchte er sein Konto erstellen und klickt auf „Konto erstellen“.

Abbrechen Konto erstellen

TechniSmart: Anmeldung x
 https://www.technismart.de/anmeldung

Konto erstellen

Techni Smart

Ihr Name:
 E-Mail:
 Passwort:
 Passwort erneut eingeben:
 Ihr Geburtstag: 1981
 Ihr Geschlecht:

Ich bin damit einverstanden, dass meine Daten für Werbezwecke verarbeitet und auch an andere Unternehmen weitergegeben werden. Diese Einwilligung kann jederzeit auf www.technismart.de/datenrichtlinien widerrufen werden.

Abbrechen

Er kann den Anmeldevorgang nicht abschließen, denn er muss zuerst der Datenverarbeitung für Werbezwecke zustimmen.

TechniSmart: Anmeldung x
 https://www.technismart.de/anmeldung

Konto erstellen

Techni Smart

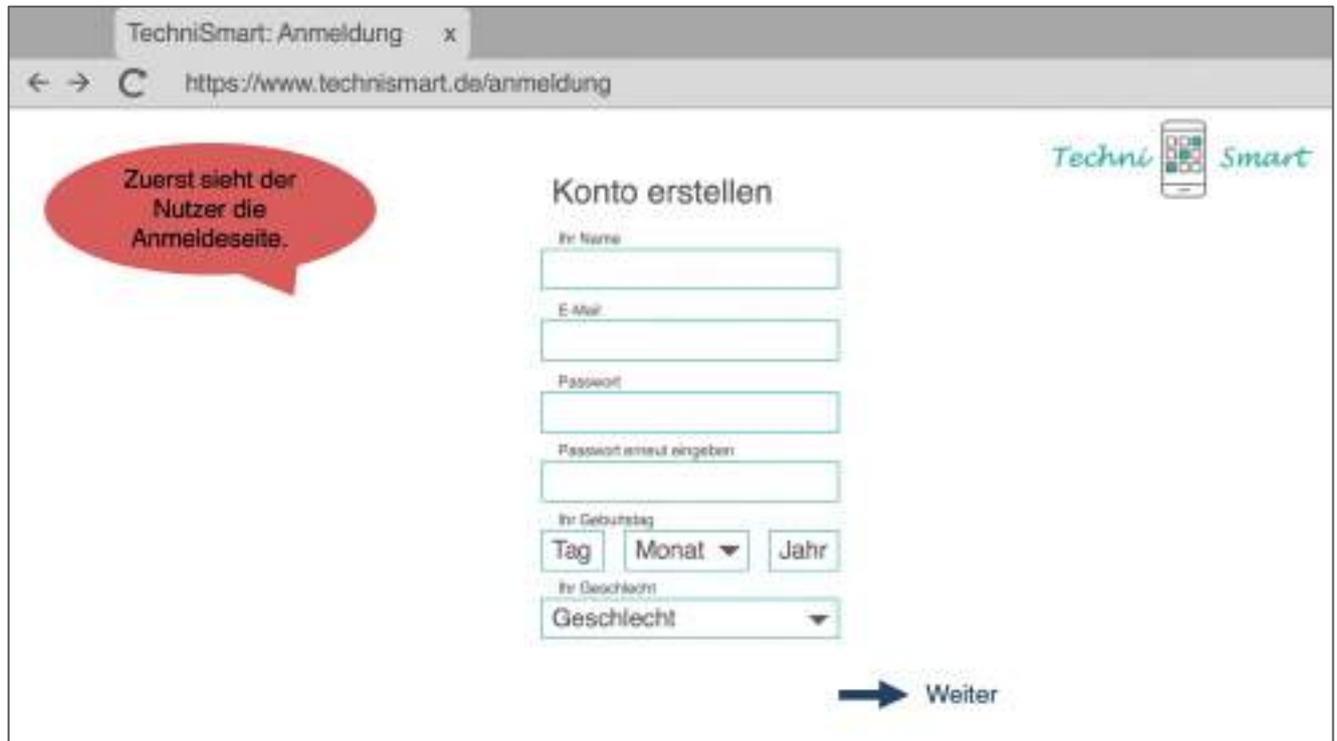
Ihr Name:
 E-Mail:
 Passwort:
 Passwort erneut eingeben:
 Ihr Geburtstag: 1981
 Ihr Geschlecht:

Ich bin damit einverstanden, dass meine Daten für Werbezwecke verarbeitet und auch an andere Unternehmen weitergegeben werden. Diese Einwilligung kann jederzeit auf www.technismart.de/datenrichtlinien widerrufen werden.

Abbrechen

Nachdem er den Haken gesetzt und eingewilligt hat, kann er fortfahren und der Anmeldevorgang ist abgeschlossen.

A.3. Mock-Ups Modell v3 (Differenzierung mit Voreinstellung und Pop-Ups)



TechniSmart: Anmeldung x
https://www.technismart.de/anmeldung

Techni Smart

Zuerst sieht der Nutzer die Anmeldeseite.

Konto erstellen

Ihr Name

E-Mail

Passwort

Passwort erneut eingeben

Ihr Geburtstag
Tag Monat Jahr

Ihr Geschlecht
Geschlecht

➔ Weiter



TechniSmart: Anmeldung x
https://www.technismart.de/anmeldung

Techni Smart

Konto erstellen

Ihr Name
Stefan Mustermann

E-Mail
stefan@mustermann.de

Passwort
●●●●●●●●

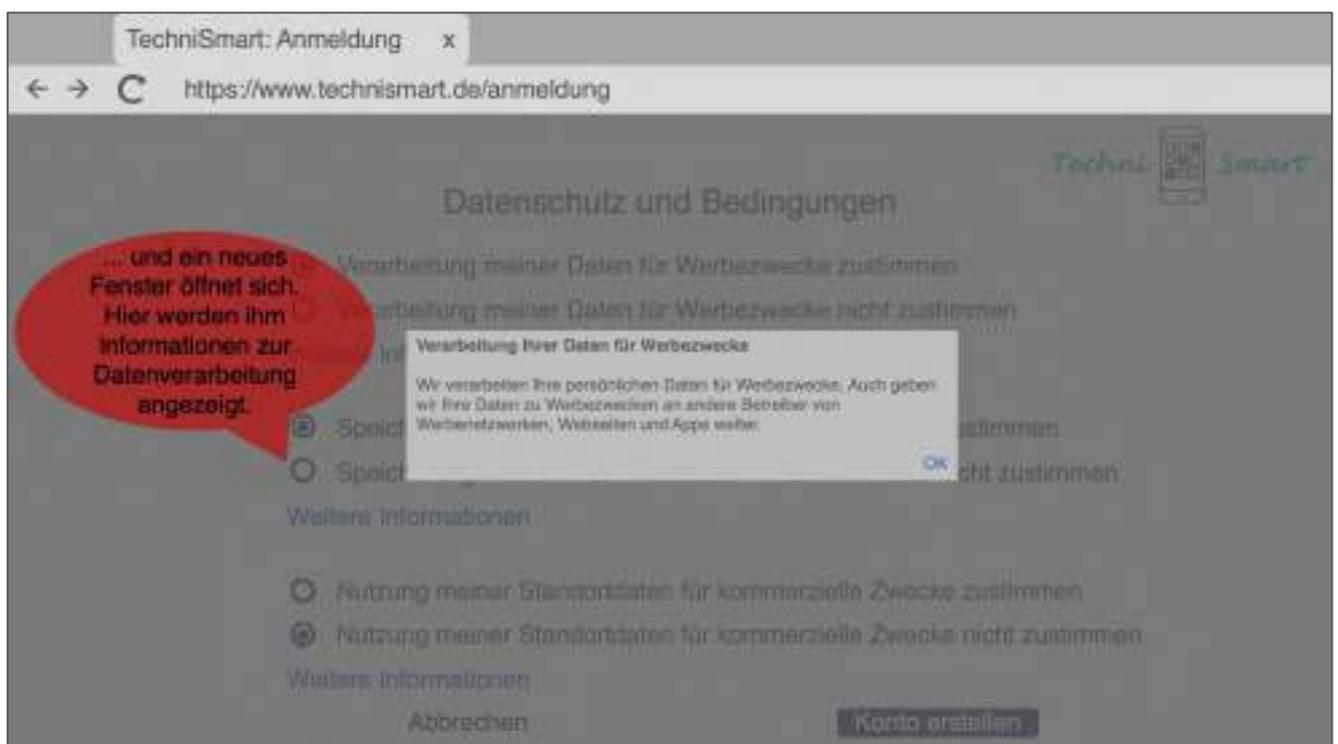
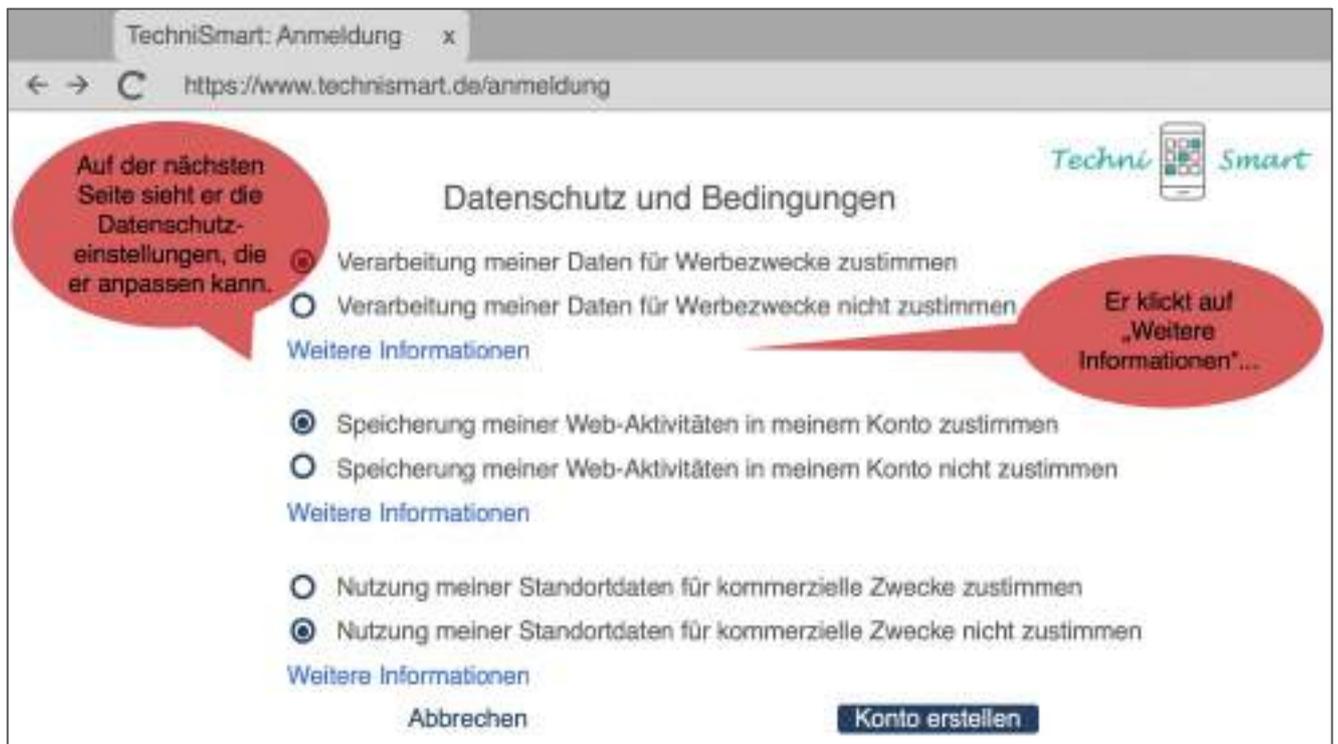
Passwort erneut eingeben
●●●●●●●●

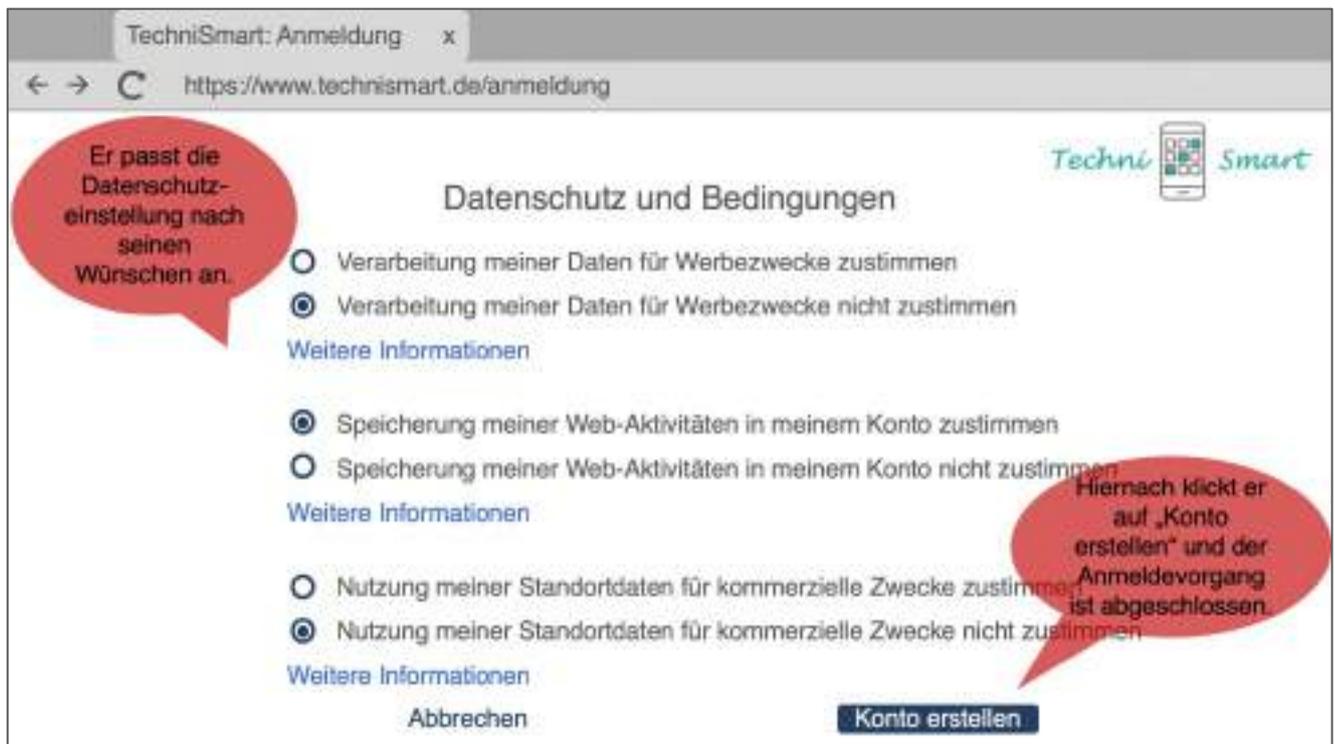
Ihr Geburtstag
22 August 1981

Ihr Geschlecht
männlich

Nachdem er seine Daten eingetragen hat, klickt er auf „Weiter“.

➔ Weiter





A.4. Mock-Ups Modell v4 (Differenzierung ohne Auswahl und mit Erläuterungstext)



TechniSmart: Anmeldung x

← → C https://www.technismart.de/anmeldung

Konto erstellen

Techni Smart

Ihr Name
Stefan Mustermann

E-Mail
stefan@mustermann.de

Passwort
●●●●●●●●

Passwort erneut eingeben
●●●●●●●●

Ihr Geburtstag
22 August 1981

Ihr Geschlecht
männlich

Verarbeitung meiner Daten für Werbezwecke zustimmen

Wir verarbeiten Ihre persönlichen Daten für Werbezwecke. Auch geben wir Ihre Daten zu Werbezwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weiter.

Speicherung meiner Web-Aktivitäten in meinem Konto zustimmen

Nachdem er seine Daten eingetragen hat, scrollt er nach unten...

TechniSmart: Anmeldung x

← → C https://www.technismart.de/anmeldung

Passwort erneut eingeben
●●●●●●●●

Ihr Geburtstag
22 August 1981

Ihr Geschlecht
männlich

Verarbeitung meiner Daten für Werbezwecke zustimmen

Wir verarbeiten Ihre persönlichen Daten für Werbezwecke. Auch geben wir Ihre Daten zu Werbezwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weiter.

Speicherung meiner Web-Aktivitäten in meinem Konto zustimmen

Mit dieser Einstellung werden Ihre Aktivitäten auf Webseiten in Ihrem Konto gespeichert. Dazu zählen Suchanfragen und verknüpfte Informationen wie der Standort. Außerdem werden Ihre Aktivitäten auf anderen Webseiten gespeichert, die unsere Dienste verwenden (z.B. einen Like-Button). Diese Informationen werden von uns verwendet, um ein möglichst umfassendes Profil von Ihnen zu erstellen und somit unsere Dienste zu personalisieren.

Nutzung meiner Standortdaten für kommerzielle Zwecke zustimmen

Wir verarbeiten Ihre Standortdaten für kommerzielle Zwecke (Werbung). Ihre Standortdaten werden zu den gleichen Zwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weitergegeben und von diesen verarbeitet. Hierbei wird eine virtuelle Karte mit Orten, die Sie mit

... hier werden die weiteren Datenverarbeitungen erläutert, die er auswählen kann.

TechniSmart: Anmeldung x

← → C https://www.technismart.de/anmeldung

22 August 1981

Ihr Geschlecht
männlich

Techni Smart

- Verarbeitung meiner Daten für Werbezwecke zustimmen**
Wir verarbeiten Ihre persönlichen Daten für Werbezwecke. Auch geben wir Ihre Daten zu Werbezwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weiter.
- Speicherung meiner Web-Aktivitäten in meinem Konto zustimmen**
Mit dieser Einstellung werden Ihre Aktivitäten auf Webseiten in Ihrem Konto gespeichert. Dazu zählen Suchanfragen und verknüpfte Informationen wie der Standort. Außerdem werden Ihre Aktivitäten auf anderen Webseiten gespeichert, die unsere Dienste verwenden (z.B. einen Like-Button). Diese Informationen werden von uns verwendet, um ein möglichst umfassendes Profil von Ihnen zu erstellen und somit unsere Dienste zu personalisieren.
- Nutzung meiner Standortdaten für kommerzielle Zwecke zustimmen**
Wir verarbeiten Ihre Standortdaten für kommerzielle Zwecke (Werbung). Ihre Standortdaten werden zu den gleichen Zwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weitergegeben und von diesen verarbeitet. Hierbei wird eine private Karte mit Orten, die Sie mit Ihren angemeldeten Geräten besuchen, erstellt, selbst wenn Sie gerade keines unserer Produkte nutzen.

Abbrechen Konto erstellen

Der Nutzer scrollt bis zum Ende der Seite.

TechniSmart: Anmeldung x

← → C https://www.technismart.de/anmeldung

22 August 1981

Ihr Geschlecht
männlich

Techni Smart

- Verarbeitung meiner Daten für Werbezwecke zustimmen**
Wir verarbeiten Ihre persönlichen Daten für Werbezwecke. Auch geben wir Ihre Daten zu Werbezwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weiter.
- Speicherung meiner Web-Aktivitäten in meinem Konto zustimmen**
Mit dieser Einstellung werden Ihre Aktivitäten auf Webseiten in Ihrem Konto gespeichert. Dazu zählen Suchanfragen und verknüpfte Informationen wie der Standort. Außerdem werden Ihre Aktivitäten auf anderen Webseiten gespeichert, die unsere Dienste verwenden (z.B. einen Like-Button). Diese Informationen werden von uns verwendet, um ein möglichst umfassendes Profil von Ihnen zu erstellen und somit unsere Dienste zu personalisieren.
- Nutzung meiner Standortdaten für kommerzielle Zwecke zustimmen**
Wir verarbeiten Ihre Standortdaten für kommerzielle Zwecke (Werbung). Ihre Standortdaten werden zu den gleichen Zwecken an andere Betreiber von Werbenetzwerken, Webseiten und Apps weitergegeben und von diesen verarbeitet. Hierbei wird eine private Karte mit Orten, die Sie mit Ihren angemeldeten Geräten besuchen, erstellt, selbst wenn Sie gerade keines unserer Produkte nutzen.

Abbrechen Konto erstellen

Er passt die Datenschutzeinstellungen nach seinen Wünschen an.

Hier nach klickt er auf „Konto erstellen“ und der Anmeldevorgang ist abgeschlossen.

A.5. Fragestellungen Zusatzfunktionen

Stellen Sie sich vor, ein Dienst würde Ihnen anbieten, Ihnen **regelmäßig Erinnerungen zu Datenschutzeinstellungen** zu senden.

Wie fänden Sie eine solche Erinnerungsfunktion?

- <1> Sehr gut
- <2> Gut
- <3> Weder gut noch schlecht
- <4> Schlecht
- <5> Sehr schlecht
- <997> Weiß nicht

Damit Verbraucherinnen und Verbraucher ihre Daten **bei einem Anbieter** einsehen und entsprechend ihrer Wünsche anpassen können, bieten manche Anbieter eine **zentrale Seite innerhalb des Nutzerkontos** an. Auf dieser Seite wird kompakt zusammengefasst, welche Daten verwendet werden und es wird ermöglicht, Daten zu löschen und zu ergänzen sowie die Einstellungen zu ändern.

Wie finden Sie eine solche Seite?

- <1> Sehr gut
- <2> Gut
- <3> Weder gut noch schlecht
- <4> Schlecht
- <5> Sehr schlecht
- <997> Weiß nicht

Stellen Sie sich bei dieser zentralen Seite vor, es gäbe eine Funktion, mit der Sie **mit einem Klick** alle Datenschutzeinstellungen für diesen Anbieter pauschal **ein- und ausschalten** könnten.

Wie gut oder schlecht fänden Sie eine solche Funktion?

- <1> Sehr gut
- <2> Gut
- <3> Weder gut noch schlecht
- <4> Schlecht
- <5> Sehr schlecht
- <997> Weiß nicht

Neben zentralen Seiten, die im Nutzerkonto einzelner Anbieter Datenschutzinformationen bereitstellen und Einstellungen ermöglichen, könnte auch eine **übergeordnete Seite (Portal)** entwickelt werden, die die Datenschutzinformationen und Einstellungsmöglichkeiten **mehrerer Anbieter** bündelt. Wie fänden Sie eine solche übergeordnete Seite (Portal)?

- <1> Sehr gut
- <2> Gut

<3>	Weder gut noch schlecht
<4>	Schlecht
<5>	Sehr schlecht
<997>	Weiß nicht

Informationen zu Datenverarbeitungen, d.h. die **Datenschutzerklärungen** von Webseiten, werden meistens als Texte dargestellt. Es wäre jedoch denkbar, dass man die textlichen Informationen um **kleine Bilder** (Piktogramme bzw. Icons) ergänzt.

Wie fänden Sie solche Bilder?

<1>	Sehr gut
<2>	Gut
<3>	Weder gut noch schlecht
<4>	Schlecht
<5>	Sehr schlecht
<997>	Weiß nicht

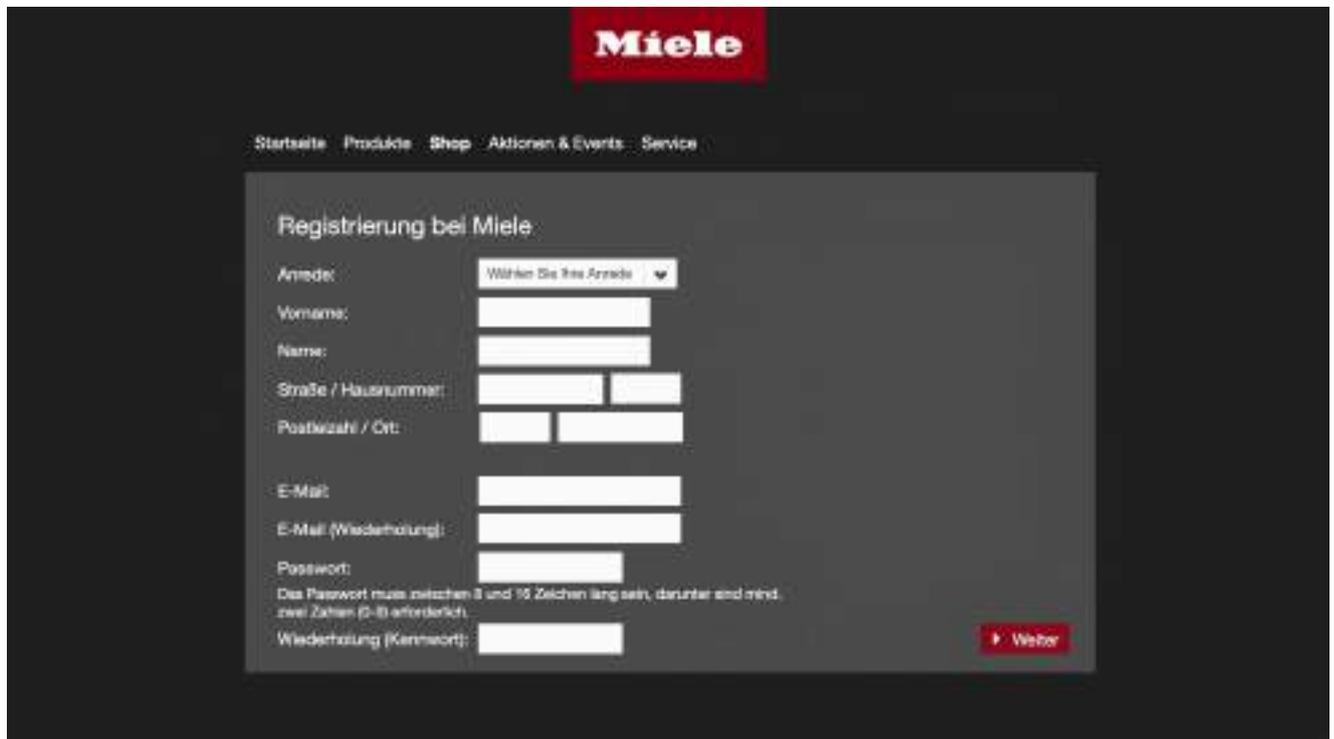
Es wäre auch denkbar, dass man die Datenschutztexpte durch sogenannte „One-Pager“ ergänzt. Das sind einfache, konzentrierte Informationen über die wesentlichen Datenverarbeitungen auf einer Seite.

Wie fänden Sie einen solchen One-Pager?

<1>	Sehr gut
<2>	Gut
<3>	Weder gut noch schlecht
<4>	Schlecht
<5>	Sehr schlecht
<997>	Weiß nicht

Anhang B: Befragungskonzept Praxistest Miele

B.1. Screenshots



The screenshot shows the Miele registration page. At the top, the Miele logo is displayed in a red box. Below it, a navigation menu includes 'Startseite', 'Produkte', 'Shop', 'Aktionen & Events', and 'Service'. The main content area is titled 'Registrierung bei Miele' and contains the following fields:

- Arbeitsort: A dropdown menu with the text 'Wählen Sie Ihre Arbeitsort' and a downward arrow.
- Vorname: A text input field.
- Name: A text input field.
- Straße / Hausnummer: Two adjacent text input fields.
- Postleitzahl / Ort: Two adjacent text input fields.
- E-Mail: A text input field.
- E-Mail (Wiederholung): A text input field.
- Passwort: A text input field with a note below it: 'Das Passwort muss zwischen 8 und 16 Zeichen lang sein, darunter sind mind. zwei Zahlen (0-9) erforderlich.'
- Wiederholung (Kenneort): A text input field.

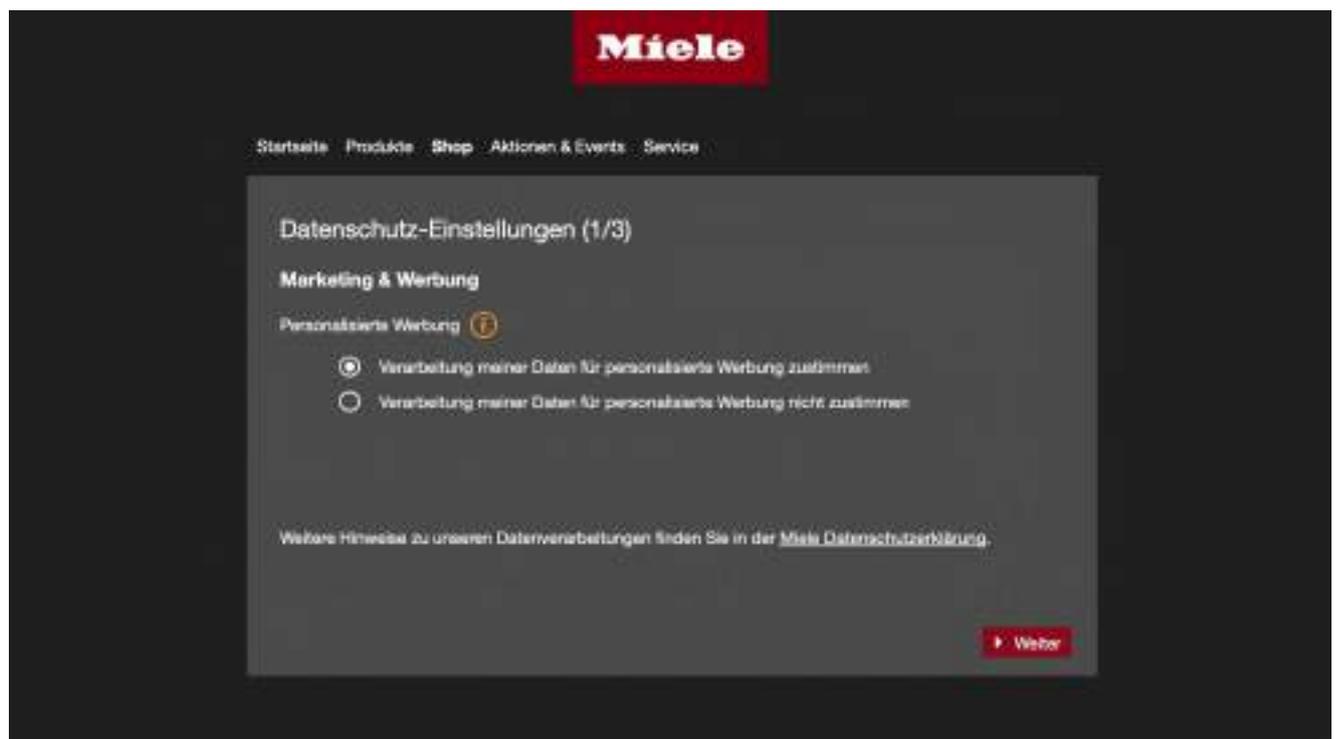
A red button labeled 'Weiter' is located at the bottom right of the registration form.

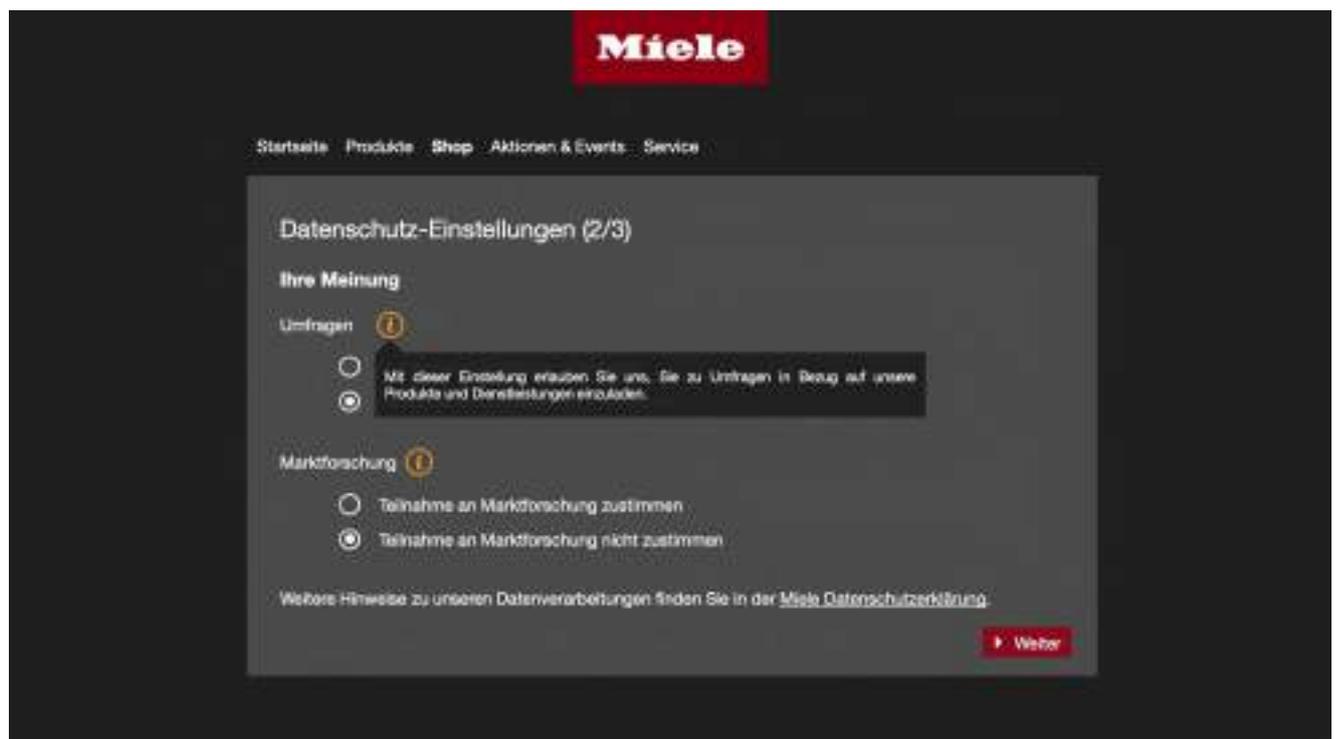
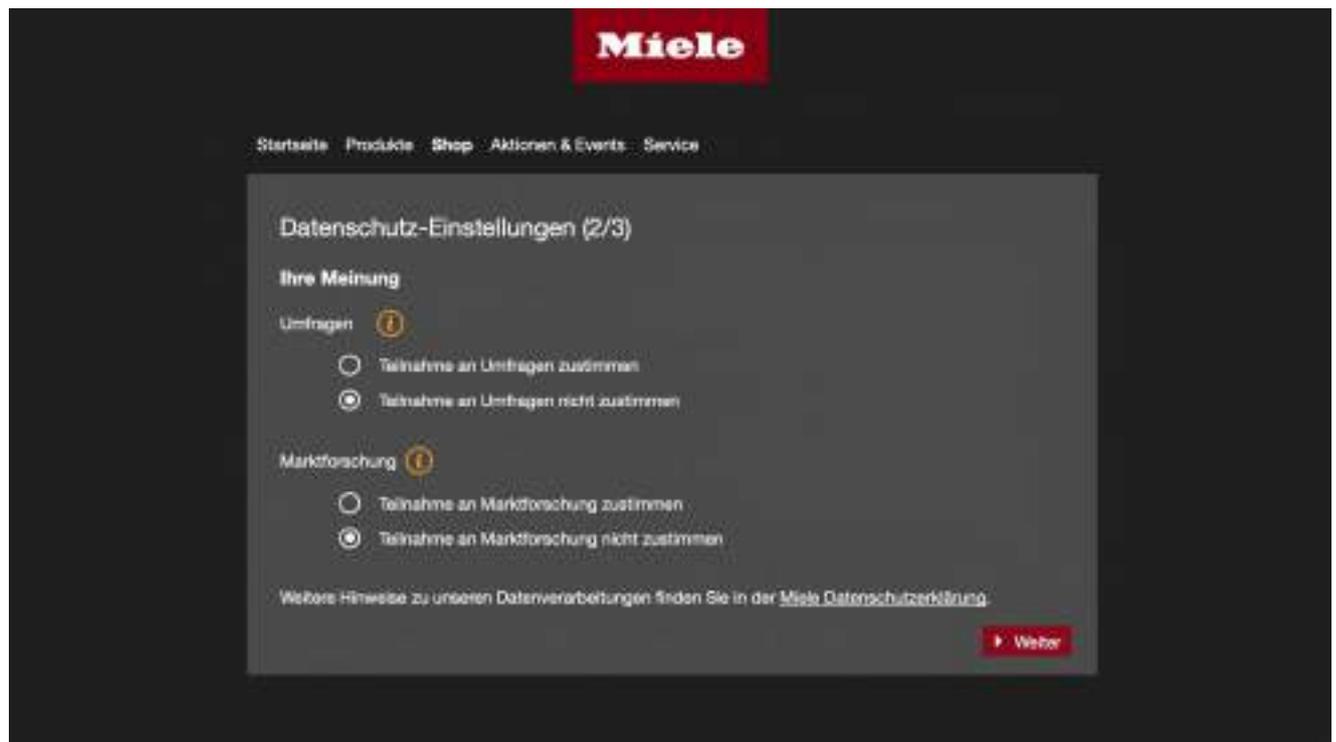


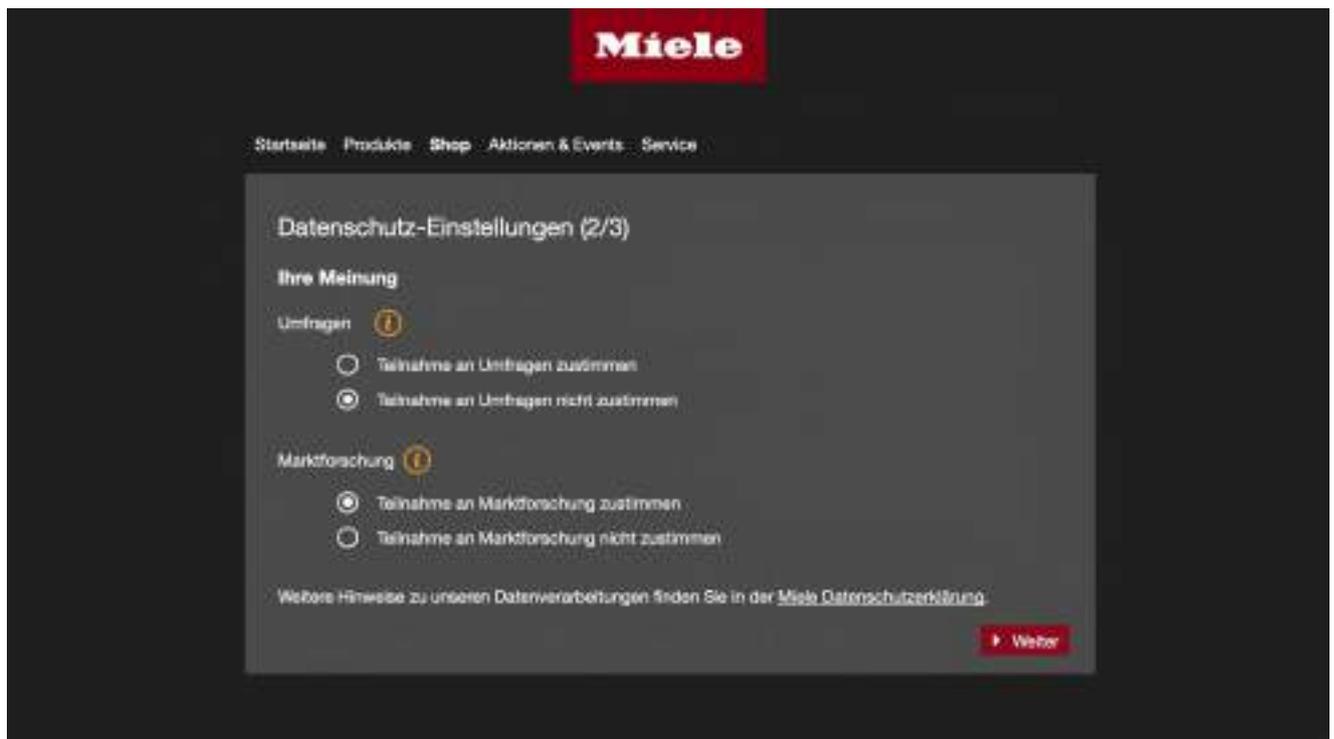
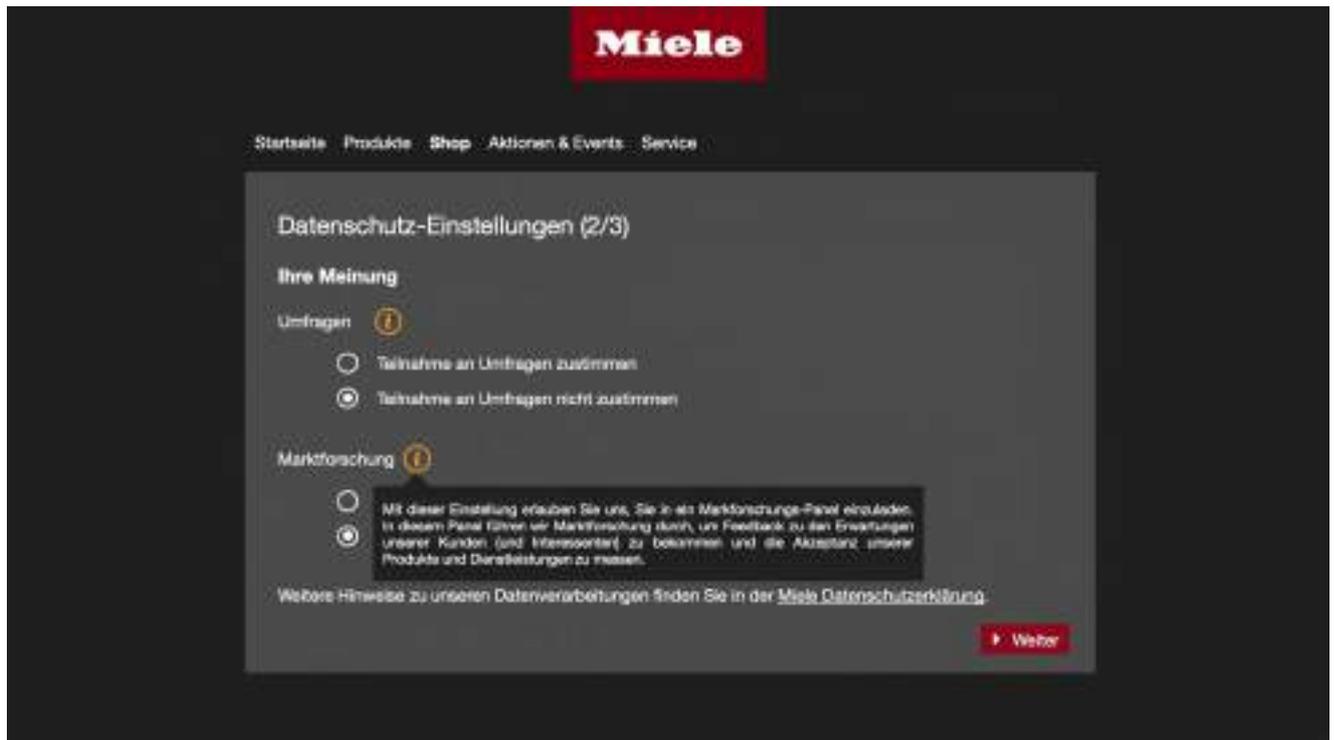
The screenshot shows the Miele privacy settings page. At the top, the Miele logo is displayed in a red box. Below it, a navigation menu includes 'Startseite', 'Produkte', 'Shop', 'Aktionen & Events', and 'Service'. The main content area is titled 'Datenschutz-Einstellungen (1/3)' and contains the following sections:

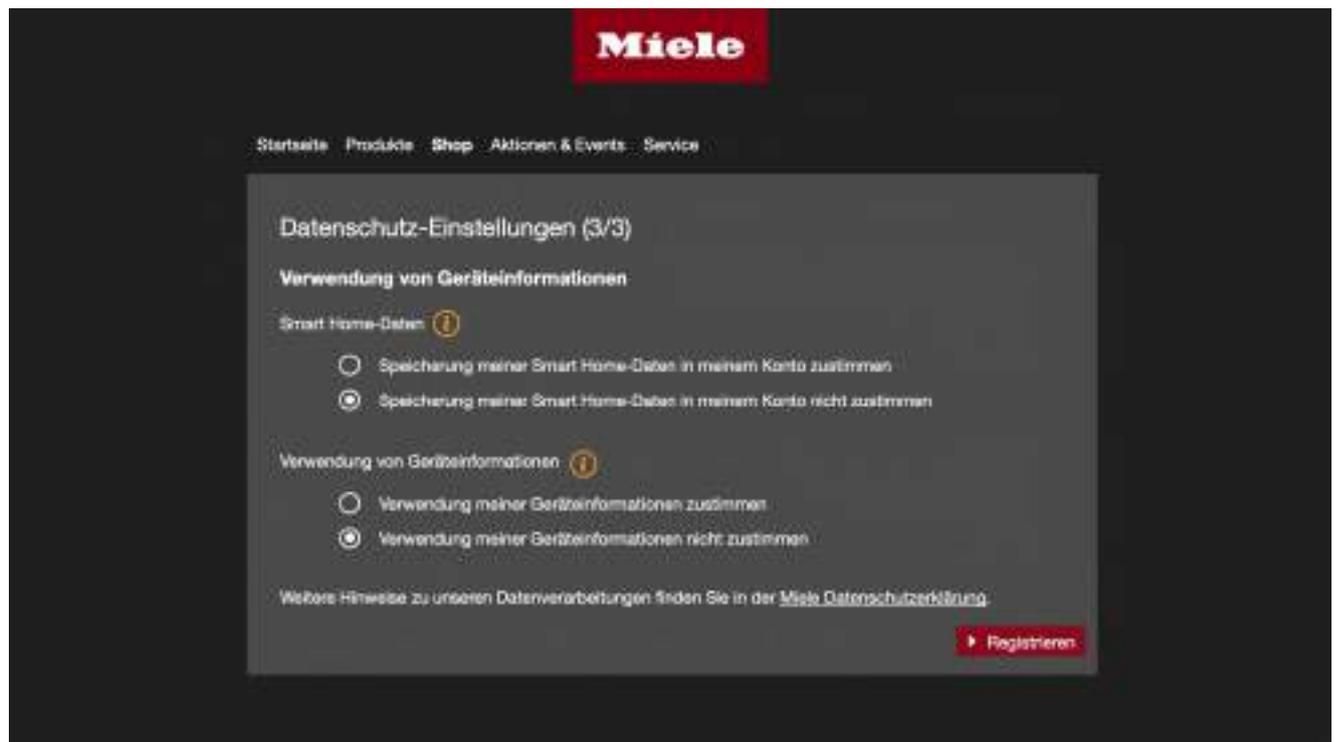
- Marketing & Werbung**
- Personalisierte Werbung** (with an information icon):
 - Verarbeitung meiner Daten für personalisierte Werbung **zustimmen**
 - Verarbeitung meiner Daten für personalisierte Werbung **nicht zustimmen**

Below the settings, there is a link: 'Weitere Hinweise zu unseren Datenverarbeitungen finden Sie in der [Miele Datenschutzerklärung](#).' A red button labeled 'Weiter' is located at the bottom right of the settings page.









Miele

Startseite Produkte Shop Aktionen & Events Service

Datenschutz-Einstellungen (3/3)

Verwendung von Geräteinformationen

Smart Home-Daten ⓘ

- Speicherung meiner Smart Home-Daten in meinem Konto zustimmen
- Speicherung meiner Smart Home-Daten in meinem Konto nicht zustimmen

Verwendung von Geräteinformationen ⓘ

Mit dieser Erstellung erlauben Sie die Verwendung von Geräteinformationen, um Sie bei wiederholter Nutzung unserer Dienste wiederzuerkennen. Zu den Geräteinformationen zählen Ihr Modellname sowie Seriennummern. Hierdurch wird die Funktionalität unserer Dienste verbessert und Ihr Gerät kann anwendungsübergreifend verfolgt werden.

Weitere Hinweise zu unseren Datenverarbeitungen finden Sie in der [Miele Datenschutzerklärung](#).

[▶ Registrieren](#)

Miele

Startseite Produkte Shop Aktionen & Events Service

Datenschutz-Einstellungen (3/3)

Verwendung von Geräteinformationen

Smart Home-Daten ⓘ

- Speicherung meiner Smart Home-Daten in meinem Konto zustimmen
- Speicherung meiner Smart Home-Daten in meinem Konto nicht zustimmen

Verwendung von Geräteinformationen ⓘ

- Verwendung meiner Geräteinformationen zustimmen
- Verwendung meiner Geräteinformationen nicht zustimmen

Weitere Hinweise zu unseren Datenverarbeitungen finden Sie in der [Miele Datenschutzerklärung](#).

[▶ Registrieren](#)

B.2. Fragebogen zum Modell

1. Wie beurteilst Du das neue Miele Datenschutz-Management insgesamt?

- <1> Sehr gut
- <2> Gut
- <3> Weder gut noch schlecht
- <4> Weniger gut
- <5> Schlecht

2. Bitte nenne uns die Gründe, weshalb du das neue Miele-Datenschutz-Management nicht so gut findest.

< Wenn Frage 1 = „weniger gut“ oder „schlecht“ >

< Offenes Textfeld >

3. Wie einfach oder kompliziert findest Du das neue Miele Datenschutz-Management?

- <1> Sehr einfach
- <2> Einfach
- <3> Weder einfach noch kompliziert
- <4> Kompliziert
- <5> Sehr kompliziert

4. Bitte nenne uns Gründe, weshalb Du das neue Miele Datenschutz-Management eher kompliziert findest.

< Wenn Frage 3 = „kompliziert“ oder „sehr kompliziert“ >

< Offenes Textfeld >

5. Im neuen Miele Datenschutz-Management kannst du Einstellungen zu Marketing & Werbung, Deiner Meinung (Umfragen) und Geräteinformationen vornehmen und so die Datennutzung wunschgemäß anpassen. Dies ist bisher noch nicht möglich. Sind diese neuen Einstellungsmöglichkeiten aus deiner Sicht eine Verbesserung?

- <1> Ja (bitte kurz begründen): < Offenes Textfeld >
- <2> Nein (bitte kurz begründen): < Offenes Textfeld >

6. Wenn es das neue Miele Datenschutz-Management in der Realität bereits gäbe, würdest du es dann nutzen?

- <1> Ja, mit Sicherheit
- <2> Ja, wahrscheinlich
- <3> Weiß (noch) nicht
- <4> Nein, wahrscheinlich nicht
- <5> Nein, mit Sicherheit nicht

7. Inwieweit stimmst du der folgenden Aussage zu: Die Gestaltung des neuen Miele Datenschutz-Managements bietet mir die Möglichkeit, diverse Einstellungen an meine individuellen Bedürfnisse und Anforderungen anzupassen.

- <1> Stimme voll und ganz zu
- <2> Stimme zu
- <3> Weder noch
- <4> Stimme nicht zu
- <5> Stimme überhaupt nicht zu

8. Bitte nenne uns Gründe, weshalb du der Meinung bist, die Einstellungen nicht an deine individuellen Bedürfnisse und Anforderungen anpassen zu können.

< Wenn Frage 7 = „Stimme nicht zu“ oder „Stimme überhaupt nicht zu“ >

< Offenes Textfeld >

9. Glaubst du, dass das neue Miele Datenschutz-Management vertrauenswürdig ist?

- <1> Stimme voll und ganz zu
- <2> Stimme zu
- <3> Weder noch
- <4> Stimme nicht zu
- <5> Stimme überhaupt nicht zu

10. Wie informiert fühlst du dich nach Nutzung des neuen Miele Datenschutz-Managements darüber, wie Miele mit deinen Daten umgeht?

- <1> Sehr gut informiert
- <2> Gut informiert
- <3> Weder gut noch schlecht informiert
- <4> Nicht gut informiert
- <5> Überhaupt nicht gut informiert

11. Bitte nenne uns die Gründe, aus denen du dich nicht gut informiert fühlst.

< Wenn Frage 10 = „Nicht gut informiert“ oder „Überhaupt nicht gut informiert“ >

< Offenes Textfeld >

Anhang C: Befragungskonzept Praxistest Telekom

Hinweis: Die vorgestellte Befragung war Teil einer größeren Befragung der Telekom zu anderen Aspekten, die unabhängig von der Forschungsfrage zum Datenschutzmanagement im Nachhinein waren. Diese anderen Aspekte und zugehörigen Fragestellungen werden im Folgenden nicht abgedruckt.

C.1. Version A (Status Quo)

<Einleitung>

Hier sehen Sie die Möglichkeit, Einstellungen am InfoService vorzunehmen.

Bitte schauen Sie sich diese Seite bitte aufmerksam an. Im Folgenden würden wir gerne Ihre Meinung dazu erfahren.



Hier sehen Sie wieder einige Aussagen zu den Einstellungsmöglichkeiten des Telekom InfoService.

Bitte geben Sie jeweils an, wie sehr die Aussage zutrifft.

Die Einstellungsmöglichkeiten des Telekom InfoService	(1) Trifft voll und ganz zu	(2)	(3)	(4)	(5) Trifft ganz und gar nicht
schaffen Vertrauen					
bieten mir einen Mehrwert					
sind klar und übersichtlich					
sind hilfreich					
sind verständlich					
bieten mir die Möglichkeit, die Einstellungen an meine individuellen Bedürfnisse anzupassen					

C.2. Version B (Datenschutz-Cockpit)

<Einleitung>

Hier sehen Sie die Möglichkeit, Einstellungen am InfoService vorzunehmen.

Bitte schauen Sie sich diese Seite aufmerksam an. Im Folgenden würden wir gerne Ihre Meinung dazu erfahren.



Hier sehen Sie wieder einige Aussagen zu den Einstellungsmöglichkeiten des Telekom InfoService.

Bitte geben Sie jeweils an, wie sehr die Aussage zutrifft.

Die Einstellungsmöglichkeiten des Telekom InfoService	(1) Trifft voll und ganz zu	(2)	(3)	(4)	(5) Trifft ganz und gar nicht
schaffen Vertrauen					
bieten mir einen Mehrwert					
sind klar und übersichtlich					
sind hilfreich					
sind verständlich					
bieten mir die Möglichkeit, die Einstellungen an meine individuellen Bedürfnisse anzupassen					