1. Einleitung

„Daten sind der Rohstoff des 21. Jahrhunderts“[1], sagte die ehemalige Bundeskanzlerin Angela Merkel bei der internationalen Konferenz *Global Solution Summits* 2018 in Berlin. In ähnlicher Weise definierten schon andere Politiker, Medien[2] und Unternehmer[3] den Wert von personenbezogenen Daten durch das digitale Zeitalter. Immer mehr Unternehmen sammeln und verarbeiten Daten Ihrer Kunden und nutzen diese für diverse Geschäftszwecke. Dabei steigt der Einsatz *automatisierter Entscheidungsfindungen*, die es ermöglicht, Daten automatisiert zu verarbeiten.[4] Zu den ähnlichen Techniken gehört das „Profiling“ und „Scoring“. Diese werden genutzt, um bestimmte Vorhersagen und Wahrscheinlichkeiten einer Person anhand seiner personenbezogenen Daten zu treffen.

Versicherungsunternehmen nutzen diese technologischen Möglichkeiten, um die Beitragshöhe der Hausratversicherung berechnen zu lassen.[5] Dabei mussten Kunden für den Abschluss einer solchen Versicherung diverse Daten von sich preisgeben. Deutschlandweit besitzen knapp 50 Millionen Kunden eine Hausratversicherung und unterlagen somit schon einer automatisierten Entscheidungsfindung.[6] Auf Seiten der Versicherung ist die Sparte der Hausratsversicherung ein lohnenswertes Geschäft, mit dem sie jährlich Millionen Euro Umsatz generieren.[7] Die zunehmende Verarbeitung personenbezogener Daten bietet aber nicht nur wirtschaftliche Vorteile, sie birgt auch Risiken in Bezug auf Macht und Privatsphäre (Mahieu et al., 2017). Durch die steigende Datennachfrage und Komplexität der Berechnung verlieren Betroffene oft den Überblick über die Datensammlung und -verarbeitung. Die Folgen: Betroffene leiden unter einem Kontrollverlust ihrer eigenen Daten und beklagen sich über fehlende Transparenz seitens der Verantwortlichen.[8]

[1] https://www.dr-datenschutz.de/merkel-datensteuer-ist-das-zentrale-gerechtigkeitsthema-der-zukunft/
[2] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
[3] https://www.giga.de/unternehmen/intel/news/ein-selbstfahrendes-auto-erzeugt-4.000-gigabyte-daten-am-tag/
[4] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_de
[5] https://deinedatendeinerechte.de/glossary/automatisierte-entscheidung/
[6] https://de.statista.com/statistik/daten/studie/266295/umfrage/versicherungen-besitz-einer-hausratversicherung-in-deutschland/
[7] https://www.procontra-online.de/bilderstrecke/date/2021/01/diese-hausratversicherer-kassierten-gross-ab/seite/3/album/1333/
[8] https://www horizont net/marketing/nachrichten/studie-zu-ein-jahr-dsgvo-jeder-dritte-deutsche-glaubt-die-kontrolle-ueber-seine-daten-verloren-zu-haben-175060

Dies erkannte auch die Europäische Union[9] und führte daraufhin die Datenschutzgrundverordnung (DSGVO) ein. Das Ziel war es, die Rechte der Betroffenen zu stärken und das Vertrauen in die Datenverarbeitung aufzubauen (Dexe et al., 2017). Dafür wurden Verantwortliche, die personenbezogene Daten sammeln, verpflichtet, diese rechtmäßig, transparent, richtig und „für die betroffene Person [in] nachvollziehbare[r] Weise" (Art. 5 Abs. 1 DSGVO) zu verarbeiten. Durch das Auskunftsrecht in Artikel 15 DSGVO wurde dem Betroffenen selbst das Recht gegeben zu überprüfen, ob sich Verantwortliche an die DSGVO halten (Dexe et al., 2017). Diese besagt, dass Betroffene Auskunft über ihre personenbezogenen Daten anfordern können, die die Verantwortlichen über sie gespeichert haben. Falls die Daten automatisiert verarbeitet wurden, müssen die Verantwortlichen „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung […]" (Art. 15 abs. 1h DSGVO) preisgeben. Damit gibt die DSGVO dem Betroffenen ein Instrument zur Kontrolle der Datenerhebung und Verarbeitung an die Hand (Jakobi et al., 2019). Dies soll ihn in die Lage versetzen, die Rechtmäßigkeit der Datenpraktiken eines Verantwortlichen zu überprüfen, nachdem diese Verarbeitung bereits begonnen hat (Mahieu et al., 2017).

Bei der Umsetzung des Auskunftsrechts gibt die DSGVO dem Verantwortlichen lediglich vor, die Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form" (Art. 12 Abs. 1 Satz 1 DSGVO) und in einer klaren und einfachen Sprache zu übermitteln. Eine Prozessbeschreibung oder Handlungsempfehlung ist nicht vorgegeben. Außerdem fehlt es an Umsetzungsvorgaben seitens Datenschutzbehörden oder Gerichtsurteilen. Für Verantwortliche bringt dieser neue Rahmen jedoch Unsicherheit hinsichtlich der Anforderungen an die Einhaltung der Verordnung mit sich (Jakobi et al., 2019). Da Verantwortliche außerdem das Recht haben, die Auskunft aufgrund diverser (legitimer) Gründe zu beschränken (§29 Abs. 1 BDSG), stellt sich an dieser Stelle die Frage, wie das Recht in der Praxis angewendet wird (Dexe et al., 2017). Die rechtliche Unklarheit hat zur Folge, dass Verantwortliche den Auskunftsprozess in unterschiedlicher Art und Weise erfüllen und die Antworten qualitativ unterschiedlich ausfallen. Empirische Studien zu Auskunftsanträgen von Mahieu et al. (2017) und Norris, et al. (2017) bestätigen diese Annahme. Die Teilnehmer der Studien empfanden das Auskunftsrecht als nicht effektiv genug, „*um Transparenz über die Verarbeitung ihrer eigenen*

[9] https://dsgvo-gesetz.de/erwaegungsgruende/nr-9/ Satz 1

personenbezogenen Daten zu erhalten." (Mahieu et al., 2017). Von einem leichten und transparenten Auskunftsprozess, wie die DSGVO vorschreibt, kann also nicht die Rede sein.

Die folgende Bachelorarbeit beschäftigt daher sich mit dem Auskunftsrecht in der Versicherungsbranche. Da Versicherungen immaterielle Dienstleistungen anbieten, die erst in der Zukunft geliefert werden können, sind diese auf ein vertrauensvolles Verhältnis mit ihren Kunden angewiesen (Dexe et al., 2017). Deshalb sprechen Experten aus der Branche auch von einem „*Geschäft mit dem Vertrauen*“ (Dexe et al., 2017). Um dies zu erreichen, müssen sie ihre Produkte und Dienstleistungen transparent zur Verfügung stellen. Der Fokus der Arbeit liegt aus den folgenden Gründen auf Hausratversicherungen. Hausratversicherungen werden von diversen Markteilnehmern angeboten, sodass eine Vielzahl separater Antworten erwartet werden kann. Zudem ist die Hausratversicherung eine relativ einfache Form der Versicherung. Der Vertragsaufbau ist über verschiedene Dienstleister hinweg homogen aufgebaut, weshalb eine optimale Vergleichbarkeit möglich ist. Darüber hinaus ist die Hausratversicherung nahezu allgegenwärtig und in Besitz von vielen Wohnungs- und Hauseigentümern, was die Rekrutierung von Freiwilligen erleichtert. Obendrein basieren die Informationen über die Hausratsversicherung nicht auf sensiblen Daten, wie beispielsweise der Gesundheit, was die Rekrutierung ebenfalls erleichtert, da die Bereitschaft der Datenpreisgabe für die Studie größer ist. Aufgrund der steigenden Datennachfrage und Komplexität der Berechnung steigt aber auch die gesellschaftliche Relevanz des Themas. Betroffene sollten durch das Auskunftsrecht in der Lage sein, die Berechnung der Hausratversicherung nachzuvollziehen.

Die Forschungsfrage lautet daher: Inwieweit werden die datenschutzrechtlichen Vorgaben zum Auskunftsrecht über automatisierte Entscheidungsfindungen bei Hausratversicherungen eingehalten? Dabei sollen folgende Fragen beantwortet werden:

- Werden die Vorgaben zum Auskunftsrecht eingehalten?
- Was legen Versicherungen offen, wenn Betroffene Auskunft verlangen?
- Inwieweit erfüllt das Auskunftsrecht in der Praxis ihr Ziel und
- wie kann man den Auskunftsprozess benutzerfreundlicher gestalten?

Damit das Auskunftsrecht seinen Zweck erfüllt und die Vorgaben in Art. 12 Abs. 1 DSGVO eingehalten werden, müssen klare Handlungsempfehlungen für den Auskunftsprozess

erarbeitet werden. Da das Auskunftsrecht für Betroffene gemacht wurde, empfiehlt es sich, diese an der Erarbeitung teilhaben zu lassen. Aus diesem Grund wurden für die vorliegende Bachelorarbeit elf Teilnehmer gebeten, einen Auskunftsantrag an ihre Hausratversicherung zu stellen. Dabei wurden die Teilnehmer mithilfe eines semistrukturierten Interviews nach ihrer persönlichen Meinung gefragt. Insgesamt wurden Auskunftsanträge an neun der zehn größten Versicherungen Deutschlands verschickt. Damit deckt die Studie über 90 Prozent der Hausratversicherungen in Deutschland ab.[10]

Da es der DSGVO an einer klaren juristischen Rechtsprechung für Handlungsempfehlungen zum Auskunftsprozess fehlt, betrachten Wachter et al. (2017) das Recht auf Erklärung zu automatisierten Entscheidungsfindungen eher als ein Recht auf Informationen. Temme et al. (2017) weisen zwar darauf hin, dass Algorithmen eine hohe Komplexität aufweisen können, diese könnten aber mit Hilfe von mehr Transparenz datenschutzgerechter gemacht werden. Für Dexe et al. (2020) bedeutet Transparenz jedoch kein uneingeschränkter Zugang zu allen Informationen. Vielmehr soll es dazu beitragen, dem Betroffenen die Möglichkeit zu geben zu beurteilen, ob die Verarbeitung angemessen und rechtmäßig ist. Turilli und Floridi (2009) sehen Transparenz daher nicht als ethisches Prinzip, sondern vielmehr als eine ethische Bedingung an. Dies sei auch im Sinne der Betroffenen, da diese nur eine begrenzte Anzahl an Informationen verarbeiten können (Eisenberg, 1995). Aus diesem Grund sehen Wauters et al. (2014) den Einsatz von benutzbarem Datenschutz wie Visualisierungstechniken als wichtig an, um Datenschutzinformationen übersichtlicher und kompakter darzustellen. Dazu zählen beispielsweise der Einsatz von mehrschichtigen Datenschutzerklärungen (Art. 29 Leitlinien), Policy Icons (Tschofenig et al., 2013) oder Erklärbilder und -videos (Haapio, 2014).

Die ersten Ansätze für benutzbaren und digitalen Datenschutz zeigten sich in Form von Transparency Enhancing Tools (TETs). TETs sind Tools, die dem Betroffenen ein besseres Verständnis über Datenschutz ermöglichen sollen. Zimmermann (2015) fasste Beispiele, Klassifizierungen und Instrumente zu TETs zusammen. Eines der ersten großen Ansätze für datenschutzförderndes Identitätsmanagement war das Projekt *Privacy and Identity Management for Europe* (PRIME). PRIME wurde 2004 gestartet und hatte das Ziel Lösungen zu erforschen, die es dem Betroffenen ermöglicht, eine bessere Kontrolle über seine Privatsphäre im Internet zu geben. *PRIME* und der Nachfolger *Primelife* entwickelten das erste

[10] https://www.versicherungsbote.de/id/4900429/chapter/1/Die-Marktfuhrer-im-dankbaren-Hausrat-Geschaft/

Privacy Dachboard namens *Data Track* und leiteten so zu einem erheblichen Beitrag der TET-Forschung bei. 2016 definierten Bier et al. (2016) acht technische Anforderungen an einen DSGVO-konformen Privacy Dachboard und stellten einen selbstentwickelten Privacy Dachboard namens *Privacy Insight* vor.

In der Regel setzt sich das Auskunftsecht aus zwei Teilen zusammen. Zum einen die Beantragung der Daten und zum anderen der Erhalt bzw. die Darstellung der Informationen. Internetseiten wie *datenanfragen.de* vereinfachen ein Stück weit den Prozess, indem Sie den Betroffenen ein Musterschreiben zur Verfügung stellen, dass sie nur noch ausfüllen und abschicken müssen. Diese Art der Vorgehensweise funktioniert aber nur, wenn der Verantwortliche diese Art der Auskunftsanforderung akzeptiert. Andere Verantwortliche akzeptieren den Auskunftsantrag nur über ihre eigene Internetseite per Formularschreiben oder über das Benutzerkonto, das der Betroffene beim Verantwortlichen hinterlegt hat. Die Möglichkeiten der Auskunftsanforderung unterscheiden sich daher teils erheblich voneinander.

Datenschutz-Zertifizierungsstellen wie die European Privacy Seal (EuroPriSe) bieten den Verantwortlichen die Möglichkeit an, ihre IT-basierten Dienste auf der Grundlage des europäischen Datenschutzes zu zertifizieren. EuroPriSe wurde im Jahr 2007 vom *Unabhängigen Landeszentrum für Datenschutz* (ULD) in Schleswig-Holstein gegründet und wird von der Europäischen Union gefördert. Eine weitere, vom ULD entwickelte Methode ist das Standard-Datenschutzmodell. Dieses „bietet geeignete Mechanismen, um rechtlichen Anforderungen der DSGVO in technische und organisatorische Maßnahmen zu überführen.“[11] In beiden Fällen stehen Datenschutz- und technische Aspekte im Mittelpunkt. Eine Prüfung nach der Usability wird hingegen nicht vorgenommen. Johansen und Hübner (2019) erstellten daher ein Modell zur Bewertung des Datenschutzes, das auf den EuroPriSe Kriterien beruht und ergänzten diese mit den Kriterien der Usability. Das Modell wird durch einen Usability Privacy (UP) Würfel dargestellt. Die darin enthaltenen UP-Kriterien sollen messbare Bewertungskriterien für die Benutzerfreundlichkeit liefern. Ihre Arbeit wurde 2020 in der Fachkonferenz *Symposium On Usable Privacy and Security* (SOUPS) veröffentlicht.[12]

[11] https://www.datenschutzzentrum.de/sdm/vorversionen/

[12] In SOUPS werden jährlich Veranstaltungen von Experten in den Bereichen HCI, Sicherheit und Datenschutz organisiert und neue Erkenntnisse veröffentlicht.

Einige wenige empirische Studien über die Sinnhaftigkeit und Nutzbarkeit von Auskunftsprozessen wurden schon durchgeführt. Dazu gehören unter anderem die Studien von Mahieu et al. (2017), die Mehrländerstudie von Norris et al., (2017) oder die vom Bundesministerium der Justiz und für Verbraucherschutz in Auftrag gegebene Studie bei der Untersuchung von Onlinediensten.[13] Die Studien kamen zu sehr unterschiedlichen Ergebnissen. In einigen Fällen wurde die Nichteinhaltung der Datenschutzverordnungen festgestellt. Dabei antworteten die Verantwortlichen zum Teil überhaupt nicht oder trugen bei ihren Antworten nicht zu mehr Transparenz bei (Mahieu et al. 2017). Die uneindeutigen Forschungsergebnisse zeigen, dass in diesem Bereich weiterer Forschungsbedarf besteht. Daher widmet sich die vorliegende Bachelorarbeit insbesondere auch der Frage, in welcher Form der Auskunftsprozess benutzerfreundlicher gestaltet werden kann.

In der folgenden Arbeit steht der Begriff „Betroffener" synonym für Versicherter bzw. Nutzer. Als „Verantwortlicher" sind Versicherungen bzw. Dienstleister gemeint, die Daten von Betroffenen sammeln und verarbeiten. Die begriffliche Verwendung entstammt aus der Datenschutzrechtlichen Definition.

Der theoretische Teil der Arbeit ist wie folgt aufgebaut: Zunächst wird der Begriff der Privatsphäre näher erläutert und anschließend beschrieben, in welcher Form die Privatsphäre eines Menschen verletzt werden kann. Außerdem werden die Begrifflichkeiten *personenbezogene Daten*, *Datenschutz* und *automatisierte Entscheidungssysteme* näher eingegangen und mit Beispielen beschrieben.

Der nächste Abschnitt bezieht sich auf den Datenschutz. Hier werden die historische Entwicklung des Auskunftsrechts und die für das Auskunftsrecht relevanten, gesetzlichen Rahmenbedingungen erläutert. Dabei wird insbesondere auf die Anforderungen zu automatisierten Entscheidungsfindungen eingegangen.

Die DSGVO fordert eine ethisch korrekte Nutzung von personenbezogenen Daten. Algorithmen, die persönliche Daten verarbeiten, haben jedoch diverse technische Gegebenheiten, die den ethischen Anforderungen nicht nachkommen können. Der folgende Abschnitt beschreibt daher ethische Beeinträchtigungen im Zusammenhang mit automatisierten Entscheidungsfindungen. Außerdem ist die Sichtweise zum Recht auf Erklärung

[13] https://bit.ly/3DAXF77

automatisierter Entscheidungsfindungen in der DSGVO Gegenstand zahlreicher Diskussionen zwischen Fachleuten der IT und Rechtswissenschaft. Aus diesem Grund werden im letzten Abschnitt Argumente aus beiden Sichtweisen erläutert und abgewägt.

Die DSGVO verlangt vom Verantwortlichen, die Einhaltung der Anforderungen im Sinne des Betroffenen so einfach wie möglich zu gestalten. Dabei kann die Forschung im Bereich Usability behilflich sein. Der letzte Abschnitt des theoretischen Teils bezieht sich daher auf die Möglichkeit, wie sich der Datenschutz mithilfe der Usability benutzerfreundlicher umsetzen lässt. Als erstes werden Herausforderungen bei der Einrichtung von Usability-Funktionen in datenschutzspezifischen Angelegenheiten genannt. Anschließend werden allgemeine Usability-Attribute wiedergegeben, die zu einem nutzbaren Datenschutz beitragen können. Schließlich werden Techniken präsentiert, die für den Einsatz von benutzbarem Datenschutz verwendet werden können. Dabei unterscheiden sich die Techniken, die zur Erklärung der Verarbeitung von personenbezogenen Daten und zur Ermöglichung der Kontrolle personenbezogener Daten genutzt werden können.

In der darauffolgenden Methodologie werden die den Untersuchungsergebnissen zugrundeliegender Forschungsmethoden dargestellt. Infolgedessen werden die gesammelten Ergebnisse vorgestellt und im Kontext diskutiert. Anschließend werden im Fazit Schlüsse gezogen, um die Forschungsfrage zu beantworten und Konsequenzen und Nutzen für die Praxis gezogen.

2. Theoretische Grundlage

Der folgende Abschnitt befasst sich mit der Einordnung der Begriffe *Privatsphäre*, *personenbezogene Daten*, *automatisierte Entscheidungsfindungen* und *Datenschutz.* Außerdem werden Risiken erläutert, die im Zusammenhang mit der Privatsphäre stehen.

2.1 Privatsphäre

Der Begriff **Privatsphäre** wurde erstmals von zwei amerikanischen Bundesrichtern, Warren und Brandeis, im Jahr 1890 thematisiert. Anlass dafür waren Fotografen, die unerlaubt Fotos von einer Hochzeitsfeier schossen. Es dauerte jedoch Jahrzehnte bis das Thema in „juristischen, sozialen und wissenschaftlichen Kreisen kontrovers diskutiert“ (Politou et al., 2018) wurde.