Datenschutz und Datensicherheit von Smart Glasses

Lisa Berkemeier, Mary-Rose McGuire, Sabrina Steinmann, Christina Niemöller, Oliver Thomas, Peter Wahlen und Jannis Vogel

Mit der zunehmenden Verbreitung von mobilen Informationssystemen und dem Aufkommen neuer Technologien stehen die relevanten Stakeholder vor der Herausforderung, Aspekte des Datenschutzes und darüber hinaus der informationellen Selbstbestimmung zu erfassen und geeignete Maßnahmen zur Sicherung dieser einzuleiten. Insb. die Einführung von Smart Glasses wird hinsichtlich datenschutzrechtlicher Bedenken kontrovers diskutiert. Dieser Diskurs ist einerseits an die neuen Rahmenbedingungen für den Schutz personenbezogener Daten nach der EU-Datenschutzgrundverordnung anzupassen. Andererseits sind aufgrund der Neuheit dieser Technologie die datenschutzrechtlichen Anforderungen und möglichen Gestaltungsvorschläge für Smart-Glasses-basierte Informationssysteme zu entwickeln, für die es bisher aufgrund der Neuheit der Technologie noch an konkreten Ansätzen fehlt. Angelehnt an die Methode der Konkretisierung rechtlicher Anforderungen werden technische und organisatorische Gestaltungsvorschläge, unter der Prämisse des Datenschutzes, in Form eines Frameworks für die Konstruktion und Implementierung von Smart Glasses im betrieblichen Einsatz erarbeitet. Aus dem Framework können spezifische Datenschutzmaßnahmen für konkrete Anwendungsfälle abgeleitet werden.¹

1 Einleitung

Forschungen im Bereich Service Science haben mobile Informationssysteme als notwendiges Instrument zur Bewältigung der vielfältigen Aufgaben im Dienstleistungssektor identifiziert (Thomas et al. 2014). Insb. Smart-Glasses-basierte Informationssysteme sind zur Unterstützung von informationsintensiven Prozessen ge-

¹ Bei diesem Kapitel handelt es sich um eine überarbeitete und ergänzte Fassung des Konferenz-Beitrags „Berkemeier L, McGuire MR, Steinmann S, Niemöller C, Thomas O (2019) Datenschutzrechtliche Anforderungen an Smart-Glasses-basierende Informationssysteme in der Logistik. In: Eibl M, Gaedke, M (Hrsg) INFORMATIK 2017. Gesellschaft für Informatik, Bonn, 1037-1048. doi: 10.18420/in2017_106.“

eignet (Niemöller et al. 2016). Für die innovativen Anwendungsmöglichkeiten dieser aufstrebenden Technologie ergeben sich jedoch relevante Einschränkungen aus dem Grundrecht auf informationelle Selbstbestimmung sowie den Anforderungen des Datenschutzrechts. Der betriebliche Einsatz dieser soziotechnischen Systeme setzt eine durchgängige Nutzung über den Arbeitstag voraus. Ihnen ist immanent, dass sie bspw. Leistungen, Standort und Bewegungsprofile erfassen, zugleich aber unbeabsichtigt auch personenbezogene Daten oder Fotos von Dritten aufnehmen können. Der Einsatz solcher invasiven Technologien setzt daher voraus, dass die Eingriffsintensität so gering wie möglich ausfällt und die berechtigten Interessen der Betroffenen durch kompensatorische Maßnahmen abgesichert werden. Den rechtlichen Rahmen hierfür bildet derzeit primär das Bundesdatenschutzgesetz, das aber zunehmend durch einen europäischen Rechtsrahmen überlagert wird. Die am 24. Mai 2017 in Kraft getretene EU-Datenschutzgrundverordnung (DSGVO) ist – ebenso wie das auf dieser Basis angepasste BDSG – seit Mai 2018 anwendbar. Gemeinsamer Nenner all dieser Rechtsgrundlagen ist, dass sie die Datenhoheit und Privatsphäre der Betroffenen vor eingreifenden Technologien, wie bspw. Smart Glasses, schützen und zu diesem Zweck dem Verwender aufgeben, Vorkehrungen für die Erhebung, Speicherung und Nutzung von Daten zu treffen. Jedoch mangelt es an konkreten Maßnahmen für die Ausgestaltung, die den gesetzlichen Vorgaben Rechnung tragen.

Erste Studien evaluieren die funktionsorientierte Konstruktion von Smart-Glasses-basierten Systemen, berücksichtigen jedoch nicht explizit Anforderungen an einen umfassenden Datenschutz (Niemöller et al. 2016). Aus dieser Ausgangssituation ergeben sich die Forschungsfragen (F1) *Welche datenschutzrechtlichen Anforderungen an Smart Glasses bestehen?* und eng damit verknüpft (F2) *Wie muss ein Smart-Glasses-basierendes System gestaltet werden, um diese Anforderungen zu erfüllen?* Im Rahmen eines Design-Science-Research-Ansatzes werden daher technische und organisatorische Gestaltungsvorschläge für den betrieblichen Einsatz von Smart Glasses unter der Prämisse des Datenschutzes, in enger Zusammenarbeit mit potenziellen Adressaten des Systems, im Rahmen einer Case Study erarbeitet. Aufgrund des aktuellen Handlungsbedarfs durch erste Anwendungsfälle von Smart Glasses im Bereich der Logistik (Bechtle und SAP 2016) wurde diese als Anwendungsdomäne fokussiert. Die Erkenntnisse zu den Anforderungen an den Datenschutz von Smart-Glasses-Applikationen werden durch eine „Konkretisierung rechtlicher Anforderungen“ (KORA) strukturiert. Das zentrale Ergebnis ist ein Framework zur Identifikation von Gestaltungsvorschlägen für die Konstruktion und Implementierung eines Smart-Glasses-basierten Informationssystems.

Der Beitrag gliedert sich wie folgt: In Abschnitt 2 werden zunächst theoretische Grundlagen im Bereich Smart Glasses und Datenschutz diskutiert. In Abschnitt 3 wird die Forschungsmethode vorgestellt. In Abschnitt 4 erfolgt die Ableitung datenschutzrechtlicher Anforderungen an Smart Glasses. In Abschnitt 5 erfolgt die Ergebnispräsentation des Frameworks zur datenschutzkonformen Gestaltung eines entsprechenden Systems. In Abschnitt 6 werden die Umsetzung des Datenschutzes

durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy-by-Design und Privacy-by-Default) sowie die damit verbundenen Auswirkungen dargestellt. In Abschnitt 7 werden die Ergebnisse zusammengefasst und weiterer Forschungsbedarf aufgezeigt.

2 Stand der Wissenschaft

Der Funktionsumfang aktueller Smart-Glasses-Modelle erfasst und nutzt Daten über den Anwender und seine Umgebung. So werden Informationen und auch digitale Kommunikation, Bild und Tonaufnahmen der Umgebung, sowie die Identifikation von Personen und Gegenständen ermöglicht. Darüber hinaus werden durch weitere Sensoren Bewegungsdaten und ggfs. auch medizinische Werte des Anwenders erfasst (Niemöller et al. 2016). Smart Glasses sind auf Grund dieser Eingriffe in die Privatsphäre, sowohl des Anwenders als auch Personen in dessen Umgebung, aus Sicht des Datenschutzes den invasiven Technologien und Werkzeugen zu zuordnen. Die Erforschung entsprechender Technologien wird zumeist isoliert von konkreten Einsatzszenarien durchgeführt und fokussiert abstrakte Datenschutzkonzepte anstelle von implementierbaren Lösungen (Bélanger et al. 2011). Unter Berücksichtigung dieser Kritik ist die Integration potenzieller Anwender und konkreter Anforderungen des Datenschutzes ein essenzieller Faktor bereits im Design und der Implementierung eines Smart-Glasses-basierten Informationssystems.

Die Umsetzung des Datenschutzes im betrieblichen Kontext ist eine Kernaufgabe jedes Unternehmens, das hierfür das Bewusstsein aller Beteiligten schärfen und die Anforderungen als wichtigen Bestandteil aller Entscheidungsprozesse und Handlungen im IT und Kommunikationsbereich verankern muss (Wächter 2003). Dabei ist jedoch zu beachten, dass der tradierte Begriff des Schutzes der Privatsphäre durch den Begriff der Datensouveränität abgelöst wird. Der Einsatz dieser eingreifenden Technologien erfordert folglich eine neue Definition des Verständnisses von Datenschutz (Schwenke 2015). So gewinnt das Konstrukt der Informationsprivatheit, als das Interesse einer Person an der Einflussnahme auf Umfang und Modalitäten der Erhebung, die Kontrolle über die Verarbeitung und den Zugriff auf personenbezogene Daten durch Dritte an Bedeutung (Bélanger et al. 2011).

3 Forschungsstrategie zur Entwicklung eines Smart-Glasses-basierten Informationssystems

Das übergeordnete Forschungsziel ist die Konstruktion eines Informationssystems zur Dienstleistungsunterstützung. Zur Gestaltung des Systems selbst bei gleichzeitiger Berücksichtigung der bestehenden Konflikte mit der Informationsprivatheit der Anwender folgt die Forschungsstrategie einem iterativen Design-Science-Re-

search-Ansatz (DSR). In der klassischen DSR werden Meta-Anforderungen und Lösungskomponenten definiert und iterativ evaluiert (Hevner et al. 2004). Für eine rigorose Strukturierung der Problemdomäne und eine fortlaufende Integration neuer Erkenntnisse der Perspektiven Anwender, Entwickler und Designer in die Artefaktkonstruktion erfolgt ein iteratives Vorgehen mit den Phasen: Heuristische Suche (bestehend aus problemstrukturierenden Heuristiken sowie Artefakt-Design-Heuristiken) und Heuristische Synthese (Gregory und Muntermann 2014) (vgl. Abb. 1). Für die Systemkonzeption werden Meta-Anforderungen sowohl aus den juristischen Anforderungen, insb. der DSGVO, als auch der wirtschaftswissenschaftlichen Literatur hergeleitet und durch spezifische Anforderungen der befragten Anwender ergänzt. Die korrespondierenden Lösungskomponenten basieren hauptsächlich auf Erkenntnissen aus Experteninterviews in der Anwenderdomäne und werden erweitert durch Erkenntnisse aus der Literatur. Zur Konkretisierung der wesentlichen datenschutzrechtlichen Anforderungen aus rechtlichen Vorschriften und Literatur, wurde eine Methode aus der Problemdomäne der rechtlichen Gestaltung von IKT angewendet (vgl. Abschnitt 4.2). Für die Entwicklung der Meta-Anforderungen und Lösungskomponenten haben einzelne Methoden zur Identifikation relevanter Literatur (vgl. Abschnitt 4.4) und der Befragung von Experten (vgl. Abschnitt 4.3) Informationen generiert.

Abb. 1. Methodisches Vorgehen

Konkretisierung rechtlicher Anforderungen. Die Identifikation der relevanten rechtlichen Anforderungen sowie die sich daraus ergebenden Vorgaben an das Smart-Glasses-basierte Informationssystem erfolgen durch die Methode der Konkretisierung rechtlicher Anforderungen (KORA) basierend auf dem Vorgehen von Hammer et al. (1993) zur rechtsgemäßen Gestaltung von IKT (vgl. Abb. 2). Die Methode wurde gewählt, da KORA nicht auf eine Bewertung der rechtlichen Ausgangssituation limitiert ist, sondern auf spezifische Gestaltungsvorschläge für die technische und organisationale Umsetzung eines sozio-technischen Systems zielt (Schulz et al. 2011). Nach dem Ansatz der KORA erfolgt zunächst eine Beschreibung der konkreten rechtlichen Anforderungen. Aus diesen werden anschließend spezifische rechtliche Kriterien für die Einführung einer neuen Technologie im privatwirtschaftlichen Kontext abgeleitet. Im Einklang mit diesen Kriterien werden technische Gestaltungsziele an das System statuiert und schließlich konkrete Gestaltungsvorschläge formuliert (Hammer et al. 1993). Hinzuweisen ist darauf,

dass sich das Ziel dieses Beitrags auf die Konkretisierung der datenschutzrechtlichen Anforderungen an Smart-Glasses-basierte Systemen im betrieblichen Kontext beschränkt. Die umfassende rechtliche Beurteilung von Smart Glasses muss – nicht zuletzt vor dem Hintergrund der aktuellen Entwicklungen im Datenschutzrecht – weiteren Arbeiten vorbehalten werden.

Abb. 2. Konkretisierung rechtlicher Anforderungen

Experteninterviews. In einer Case Study mit einem globalen Logistikdienstleister wurden ein Datenschutzbeauftragter, ein Information Security Officer sowie ein Betriebsratsvorsitzender als Experten befragt. In Bezug auf die Informationsprivatheit der Anwender des Informationssystems sind insb. die Erkenntnisse des Betriebsratsvorsitzenden, als Vertreter der betroffenen Mitarbeiter, richtungsweisend. Die Fragen zum Themenkomplex Datenschutz ergeben sich aus den rechtlichen Kriterien, die sich aus dem aktuellen Rechtsrahmen (BDSG, DSGVO) sowie der Literatur spezifisch zur datenschutzrechtlichen Betrachtung in invasiven Technologien ableiten. So wurden die Experten unter anderem gefragt „*Welche Anforderungen sollten ihrer Expertise nach bei der Gestaltung eines Smart-Glasses-Systems besonders berücksichtigt werden?*“ und „*Welche konkreten Gestaltungsvorschläge leiten Sie aus den genannten Anforderungen für die Systementwicklung ab?*“. Ziel der Interviews bestand im ersten Schritt in der Vervollständigung der Problemklassen, sowie in der Ableitung von Meta-Anforderungen in Form technischer Gestaltungsziele. Darauf aufbauend wurden konkrete Gestaltungsvorschläge als Lösungskomponenten für das Systemdesign in den Interviews entwickelt. Der zu Grunde liegende Interviewleitfaden ist semi-strukturiert, um die für den iterativen Einsatz notwendige Flexibilität zu ermöglichen. Die Datenauswertung der Interviews erfolgte durch eine dokumentarische Transkription und Codierung nach Nohl (2012).

4 Ableitung datenschutzrechtlicher Anforderungen an Smart-Glasses-basierte Informationssysteme

4.1 Rechtliche Anforderungen

Vornehmlich konkretisiert die DSGVO die rechtskonforme automatisierte Datenverarbeitung, genauer: die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten (Paal et al. 2017). Personenbezogene Daten umfassen nach Art. 4 Nr. 1 DSGVO Einzelangaben über persönliche oder sachliche Verhältnisse einer

natürlichen Person. Im Fall von Datenerhebungen innerhalb von Gruppen handelt es sich weiterhin um ein persönliches Datum, wenn Rückschlüsse auf einen Einzelnen gezogen werden können (Paal et al. 2017). Ferner gibt es spezielle Regelungen hinsichtlich besonderer Arten personenbezogener Daten (bspw. Herkunft, Gewerkschaftszugehörigkeit oder Gesundheit) (vgl. Art. 4 Nr. 1, 13, 14 DSGVO). Ist die DSGVO anwendbar, werden Anforderungen an die Rechtmäßigkeit der Verarbeitung, die in der Regel die Einwilligung des Betroffenen voraussetzt (Art. 6 ff.), sowie Rechte des Betroffenen und Schutzpflichten des Verantwortlichen definiert (Art. 12 ff.), wobei die Dichte der Rechte und Pflichten jeweils von der Kategorie der erhobenen Daten und dem Zweck der Erhebung abhängen. Leitprinzipien sind dabei die Datensparsamkeit, Datentransparenz und Datensicherheit. Die nachfolgende Analyse beruht auf der Annahme, dass beim Einsatz von Smart Glasses nur sonstige Daten, also weder genetische, biometrische und Gesundheitsdaten noch sicherheitsrelevante Daten erhoben werden und dies im berechtigten Interesse des Unternehmens erfolgt.

Im Folgenden wird der Rahmen der DSGVO als Maßstab für die Strukturierung der Problemklasse Datenschutz herangezogen. Dies hat zugleich den Vorteil, dass die vorgestellte Methode aus für die Ausgestaltung in anderen Mitgliedsstaaten herangezogen werden kann. Die entsprechenden rechtlichen Anforderungen werden in [Abb. 5](#) dargestellt.

4.2 Rechtliche Kriterien

Die DSGVO ist ein Regelungsrahmen auf hohem Abstraktionsniveau. Wenngleich sie aufgrund der weiten Definition des Begriffs der „personenbezogenen Daten“ auch den Einsatz von Smart Glasses umfasst ist sie – wie Zielsetzung und Regelungssystematik belegen – im Kern auf ganz andere Fälle, insb. das Profiling zugeschnitten. Vor diesem Hintergrund bietet es sich an, für die Auswahl der relevanten rechtlichen Kriterien zur Einführung eines auf Smart-Glasses-basierten Informationssystems den ersten Befund nicht an Hand des Normtextes, sondern primär aus Erkenntnissen der Literaturrecherche abzuleiten. In der Literatur ergibt sich ein überwiegend einvernehmliches Verständnis der für IKT relevanten Ausprägungen des Datenschutzes (vgl. [Abb. 3](#)). Diese Kriterien können im Rahmen von KORA als rechtliche Kriterien und im Sinne des DSR-Ansatzes als Teilprobleme formiert werden. Eine Übersicht über die in der Fachliteratur identifizierten Konstrukte gibt [Abb. 3](#). Die acht identifizierten Kriterien werden jeweils überwiegend mindestens von zwei verschiedenen Autoren genannt und stehen in einer interdependenten Beziehung zueinander.

Konstrukte aus der Literatur	Ausprägungen der Konstrukte								
	Einwilligung	Zweckbindungsgrundsatz	Rechte auf Auskunft	---	---	---	Datenvermeidung & -sparsamkeit	Mitbestimmungsrecht	---
Thüsing et al. (2014)									
Bizer et al. (2006)	Rechtmäßigkeit	Zweckbindung	Transparenz	Datensicherheit	Erforderlichkeit	Kontrolle	---	---	---
	wirksame Einwilligung								
Hammer et al. (1993)	Entscheidungsfreiheit	Zweckbindung	Transparenz	Techniksicherung	Erforderlichkeit	Kontrolleignung	---	Anpassungsfähigkeit	Arbeits- erleichterung Werkzeug- eignung
Roßnagel (2007)	Besondere Zulassung	Zweckbindung	Transparenz	Selbst- und Systemdatenschutz	Erforderlichkeit	Kontrolle	---	Mitwirkung	---
Rechtliche Kriterien	Einwilligung	Zweckbindung	Transparenz	Datensicherheit	Erforderlichkeit	Kontrolle	Datenvermeidung und -sparsamkeit	Mitwirkung	keine Zuordnung

Abb. 3. Herleitung der rechtlichen Kriterien aus der Literatur

4.3 Ziele technischer Gestaltung

Die Ziele der technischen Gestaltung eines Smart-Glasses-basierten Informationssystems nach KORA stellen Meta-Anforderungen im Sinne der DSR-Methode dar. Diese begegnen der Problemdomäne auf Ebene der Teilprobleme und adressieren konkrete Lösungselemente.

Erkenntnisse aus der Literatur. In der Literatur wurden insg. 16 Meta-Anforderungen an die Lösungskomponenten des Datenschutzes von Smart-Glasses-basierten Informationssystemen identifiziert. Aus der DSGVO können sowohl direkte als auch implizite Anforderungen an die Gestaltung eines Smart-Glasses-basierten Systems abgeleitet werden. Im Fokus der Betrachtungen steht dabei Art. 24 i.V.m. Art. 25 DSGVO als spezifische Norm für den Datenschutz durch Technik (Paal et al. 2017). Eine Übersicht gibt [Abb. 5](#).

Erkenntnisse aus den Interviews. Im Rahmen der Experteninterviews wurden vier Meta-Anforderungen ergänzt (MA5,8,10,14) und drei Meta-Anforderungen parallel zur Literatur entwickelt (MA2,4,6). Einige Aspekte wurden mehrfach genannt oder variieren in der Formulierung oder Ausrichtung der Aussagen. Daher wurden die Aspekte in einem nächsten Schritt einheitlich als Gestaltungsziele formuliert. Auf dieser abstrakten Ebene konnten mehrere Aspekte zu einer gemeinsamen Meta-Anforderung aggregiert werden. Diese Zuordnung wird in [Abb. 4](#) dargestellt.

Aspekt	I1	I2	I3	Aggregation
Keine Aufnahmen in sozialen Räumlichkeiten	x			(MA2) Aufnahmen nur in erforderlichen Bereichen
Aufnahmen nur in vorgesehenen Bereichen	x		x	
Keine individuellen Kennzahlen erheben	x	x		(MA4) Kennzahlen dürfen nicht individualisierbar sein
Kennzahlen dürfen nicht individualisierbar sein		x		
Keine Laufleistung erfassen		x		
Erkennbarkeit von Aufnahmen	x			(MA5) Erkennbarkeit von Datenerhebungen
Erkennbarkeit von Datenerhebungen		x		
Keine Erhebung besonderer personenbezogener Daten		x	x	(MA6) Keine Verarbeitung besonderer personenbezogener Daten
Gesundheitszustand nicht erfassen		x	x	
Datenschutz von Beginn bei der Systemplanung integrieren		x	x	(MA8) Datenschutz von vornherein berücksichtigen
Mitarbeiter von Beginn einbeziehen	x			
Mitarbeiter vorab einbeziehen	x	x		(MA10) Mitarbeiter von vornherein einbeziehen
Vertrauliche Kommunikation			x	
				(MA14) Vertraulichkeit

Abb. 4. Meta-Anforderungen aus den Experteninterviews

4.4 Technische Gestaltungsvorschläge

Erkenntnisse aus der Literatur. Auffällig ist das Ungleichgewicht zwischen Meta-Anforderungen und konkreten Lösungselementen aus der Literatur. Insb. die DSGVO beschreibt die Anforderungen an die Rahmenbedingungen des Datenschutzes, geht jedoch nicht auf spezifische Aktivitäten oder Handlungsanweisungen zur Umsetzung ein. Primäre Ursache hierfür ist, dass der rechtliche Rahmen bewusst technologieneutral formuliert ist (EG 15 DSGVO), um eine rasche Anpassung der Normen an die Schnelllebigkeit entsprechender technischer Lösungen entbehrlich zu machen. So gibt es abstrakte technische und organisatorische Maßnahmen (Art. 32 DSGVO) (LK13) zur Gewährleistung der Datensicherheit, die nur teilweise im Mindestmaßnahmenkatalog spezifiziert werden (Paal et al. 2017). Die DSGVO stellt einen umfassenden Pflichtenkatalog für die Verarbeitung personenbezogener Daten auf, wobei der Umfang von der Intensität des Eingriffs abhängt. Daraus lässt sich umgekehrt die Anforderung ableiten, dass – soweit möglich – nur Daten erhoben werden sollten, die keiner der besonders geschützten Kategorien zuzuordnen sind, diese nur in dem erforderlichen Ausmaß erhoben werden und keine dauerhafte Speicherung erfolgen sollte. Die Erhebung von Daten durch ein privatwirtschaftliches Unternehmen setzt zudem eine explizite und informierte Einwilligung voraus, die von Seiten des Unternehmens zu dokumentieren ist.

Rechtliche Anforderungen	Informationelle Selbstbestimmung	Datenschutz-Grundverordnung	Beschäftigten-datenschutz	Betriebs-verfassungsrecht
Rechtliche Kriterien	(TP1) Besondere Zulassung	(TP2) Erforderlichkeit	(TP3) Zweckbindung	(TP4) Datenvermeidung und Datensparsamkeit
	(TP5) Transparenz	(TP6) Datensicherheit	(TP7) Mitwirkung	(TP8) Kontrolle
Gestaltungsziele	(MA1) Erlaubnis durch Betroffene	(MA2) Datenerhebung nur in erforderlichen Bereichen	(MA3) Datenverarbeitung ausschließlich zu einem festgelegten Zweck	(MA4) Kennzahlen dürfen nicht individualisierbar sein
	(MA6) Keine Verarbeitung besonderer personenbezogener Daten		(MA9) Meldepflicht	(MA11) Verfügbarkeit
	(MA12) Authentizität	(MA13) Integrität	(MA15) Systemseitiger Datenschutz	(MA16) Verhältnismäßigkeitsprinzip
	(MA17) Einflussnahme der Betroffenen	(MA18) Selbstkontrolle	(MA19) Eigenkontrolle	(MA20) Fremdkontrolle
Gestaltungsvorschläge	(LK3) Kontrolle	(LK5) Personenbezogene Daten anonymisieren und pseudonymisieren	(LK8) Optische Signale	(LK11) Privacy-by-design/-default
	(LK13) Inhalt der Meldepflicht	(LK14) technische und organisatorische Maßnahmen	(LK16) Förderung des Selbstdatenschutz	(LK19) Betrieblicher Datenschutzbeauftragter
			(LK18) Auskunftsrechte der Betroffenen	(LK20) Vorabkontrolle

Abb. 5. Ergebnisse der KORA, basierend auf der Literatur

Erkenntnisse aus den Interviews. In den Experteninterviews wurde diese Auslegungsfreiheit der DSGVO kritisch betrachtet. Welche Maßnahmen ausreichend sind, um dem aktuellen Stand der Datensicherheit zu entsprechen, liegt im Ermessen der Unternehmen. Dieser Konflikt verdeutlicht die Notwendigkeit freiwilliger Maßnahmen, wie die kontinuierliche Einhaltung und Auditierung angemessener Sicherheitsstandards im Sinne des Art. 32 DSGVO (LK10). In den Interviews wurden zehn Lösungskomponenten für die Problemdomäne Datenschutz herausgearbeitet (vgl. Abb. 6).

Aspekt	I1	I2	I3	Aggregation
Betriebsvereinbarung	x	x	x	(LK1) Betriebsvereinbarung
Schutzzonen			x	(LK2) Schutzzonen
Gates zur Abschaltung			x	
Freiwilligkeit individueller Kennzahlen	x			(LK6) Individuelle Kennzahlen freiwillig und persönlich
Individuelle Kennzahlen nur Mitarbeiter spiegeln	x			
Kennzahlen auf Team/ Mannschaftsebene	x			(LK7) Gruppenbezogene Kennzahlen
Optisches Signal bei Aufnahme			x	(LK8) Optische Signale
Keine Speicherung von Video- und Fotoaufnahmen		x		
Schlankere Businessgeräte			x	(LK9) Funktionsabschaltung
ISO 47001		x		(LK10) Sicherheitsstandards
Privacy-by-Design		x		(LK11) Privacy-by-Design/ Default
Gewicht möglichst gering halten		x		(LK12) Modellwahl
Funktionsweise System kommunizieren	x			(LK13) Inhalt der Meldepflicht
Zweck der Datenerhebung	x			
Inhalt der Datenerhebung	x			
Verantwortliche Stelle bekannt machen	x			
Schriftliche Erklärung aushängen		x		
Zugriffsbeschränkung	x		x	(LK14) Technische und organisatorische Maßnahmen
Interne Datenschutzorganisation		x		
Verschlüsselung			x	(LK15) Verschlüsselung
Betriebsrat entscheidet ob Aufnahmen angesehen werden dürfen	x			(LK17) Einflussnahme des Betriebsrats
Datenschutzbeauftragter	x			(LK19) Betrieblicher Datenschutzbeauftragter
Vorabkontrolle	x	x	x	(LK20) Vorabkontrolle

Abb. 6. Lösungskomponenten aus den Experteninterviews

5 Framework zur datenschutzkonformen Gestaltung von Smart-Glasses-basierten Informationssystemen

Ausgehend von den Teilproblemen, erfolgt die Zuordnung der Meta-Anforderungen und entsprechenden Lösungskomponenten, dargestellt in Abb. 7. Das entstandene Framework dient als Übersicht, welche rechtlichen Rahmenbedingungen eingehalten werden müssen und offeriert entsprechende Gestaltungsmöglichkeiten für die Konstruktion und Implementierung eines Smart-Glasses-basierten Systems. So verlangt bspw. die Erforderlichkeit der Datenerhebung (TP2), die Beschränkung der Datenerhebung auf erforderliche Bereiche (MA2). Diese Anforderung wird umgesetzt in der Errichtung von Schutzzonen (LK2).

Teilproblem (TP)		Meta-Anforderung (MA)		Lösungskomponente (LK)	
TP1	Rechtmäßigkeit/ besondere Zulassung	MA1	Erlaubnis durch Betroffene	LK1	Betriebsvereinbarung
TP2	Erforderlichkeit	MA2	Datenerhebungen nur in erforderlichen Bereichen	LK2	Schutzzonen
TP3	Zweckbindung	MA3	Datenverarbeitung ausschließlich zu einem festgelegten Zweck	LK3	Kontrolle
				LK4	Daten nach Zweck getrennt speichern
TP4	Datenvermeidung und Datensparsamkeit	MA4	Kennzahlen dürfen nicht individualisierbar sein	LK5	Anonymisieren und Pseudonymisieren
				LK6	Individuelle Kennzahlen freiwillig und persönlich
				LK7	Gruppenbezogene Kennzahlen
		MA5	Erkennbarkeit von Datenerhebungen	LK8	Optische Signale
		MA6	Keine Verarbeitung besonderer personenbezogener Daten	LK9	Funktionsabschaltung
		MA7	Datenschutzaudits	LK10	Sicherheitsstandards
TP5	Transparenz	MA8	Datenschutz von vornherein berücksichtigen	LK11	Privacy-by-Design/ Default
				LK12	Modellwahl
		MA9	Meldepflicht	LK13	Inhalt der Meldepflicht
		MA10	Mitarbeiter von vornherein einbeziehen		
TP6	Datensicherheit	MA11	Verfügbarkeit	LK14	Technische und organisatorische Maßnahmen
		MA12	Authentizität		
		MA13	Integrität		
		MA14	Vertraulichkeit	LK15	Verschlüsselung
		MA15	Systemseitiger Datenschutz	LK11	Privacy-by-Design/ Default
		MA16	Verhältnismäßigkeitsprinzip		
TP7	Mitwirkung	MA17	Einflussnahme der Betroffenen	LK17	Einflussnahme des Betriebsrats
				LK18	Auskunftsrechte des Betroffenen
TP8	Kontrolle	MA18	Selbstkontrolle	LK16	Förderung des Selbstdatenschutzes
		MA19	Eigenkontrolle	LK19	Betrieblicher Datenschutzbeauftragter
				LK20	Vorabkontrolle
				MA20	Fremdkontrolle

Abb. 7. Framework zur datenschutzrechtlichen Gestaltung eines Smart-Glasses-Systems

Passieren Smart-Glasses-Anwender diese Bereiche, erfolgt eine automatische Abschaltung des entsprechenden Sensors, wie einer Kamera, mittels gesetzter Marker. Lösungskomponenten wie diese, die auf die technologiebasierten Einschränkungen mit wiederum technischen Lösungen reagieren, verdeutlichen die Relevanz der Erforschung von Informationsprivatheit in der Wirtschaftsinformatik (Pavlou und Paul 2011) und erweitern die Möglichkeiten des Selbstdatenschutzes der Anwender durch die Nutzung entsprechender Technologien.

6 Privacy-by-Design und Privacy-by-Default

6.1 Privacy-by-Design aufgrund gesetzlicher Anordnung

Neben der Berücksichtigung des Frameworks für eine datenschutzrechtskonforme Gestaltung von Smart-Glasses-Anwendungen, muss nach gesetzlicher Anordnung der Privacy-by-Design-Ansatz bei der Konzeption und Entwicklung von Smart-Glasses-basierten Informationssystemen herangezogen werden. So verlangt Art. 25 Abs. 1 DSGVO, dass der Datenschutz durch Technikgestaltung gewährleistet wird. Hierdurch wird dem Verantwortlichen (siehe Art. 4 Nr. 7 DSGVO) die Pflicht auferlegt, die Einhaltung der Verordnung und den Schutz der Betroffenen durch die frühzeitige Implementierung geeigneter technischer und organisatorischer Maßnahmen in seine Datenverarbeitung sicherzustellen (Martini 2018). Welche konkreten Maßnahmen hier gemeint sind, lässt Art. 25 Abs. 1 DSGVO offen, als konkretes Beispiel nennt die Vorschrift lediglich die in Art. 4 Nr. 5 DSGVO legal definierte Pseudonymisierung. Klar ist aber, dass eine Maßnahme alleine nicht ausreichend ist (Hackenberg 2019). Vielmehr sind nach der Konzeption der Verordnung stets auch die Grundsätze des Art. 5 Abs. 1 DSGVO zu beachten (Hartung 2018). Eine konkrete Anleitung, Methodik oder Instrumente zur Umsetzung nennt die Verordnung indes nicht, so dass die Verantwortlichen weitgehend – mit Ausnahme des Mittels der Zertifizierung – auf sich selbst gestellt sind; sie haben somit auf der einen Seite einen weiten Gestaltungsspielraum, auf der anderen Seite besteht aber bis zu einer gerichtlichen Klärung auch erhebliche Rechtsunsicherheit (Hartung 2018).

Privacy-by-Design beschreibt dabei ein Vorgehen, bereits im Designprozess und über alle Entwicklungsphasen hinweg entsprechende datenschutzrechtliche Design-Patterns und Datensicherheitsmaßnahmen anzuwenden. Dabei zielt das entworfene Design darauf ab, mögliche Datenschutzverletzungen auf ein Minimum zu reduzieren (van Rest et al. 2014). Gelingen kann dies zum einen durch die Integration sog. Privacy-Enhancing-Technologies (PET) in die Verarbeitungsvorgänge, also solcher Technologien, die dem Schutz personenbezogener Daten verschrieben sind; zum anderen sind aber auch organisatorische Maßnahmen zur Umsetzung des Konzeptes essenziell, welche durch prozedurale Sicherungen auf eine Einhaltung datenschutzrechtlicher Prinzipien hinwirken (Martini 2018), wie etwa Schulungen, interne Kontrollen, Rollen- und Berechtigungskonzepte sowie Löschkonzepte (Hartung 2018). Dabei ist – entgegen dem Schlagwort „Privacy-by-Design“, welches sich in der Literatur in Bezug auf Art. 25 Abs. 1 DSGVO begrifflich durchgesetzt hat – nicht die Privatsphäre des Einzelnen im Sinne der Wahrnehmung der individuellen Persönlichkeitsrechte oder des Rechts auf informationelle Selbstbestimmung das primäre Schutzziel, vielmehr stellt die Vorschrift das Grundrecht auf den Schutz personenbezogener Daten in den Mittelpunkt (vgl. Art. 1 Abs. 2 DSGVO) (Baumgartner 2018).

6.2 Privacy-by-Default als weitere Konkretisierung des technisch-basierten Datenschutzes

Ein nahestehendes Konzept zum Privacy-by-Design ist Privacy-by-Default, welches in Art. 25 Abs. 2 DSGVO geregelt ist und vom Verantwortlichen datenschutzfreundliche Voreinstellungen verlangt. Diese Regelung kann als eine Konkretisierung von Art. 25 Abs. 1 DSGVO gesehen werden, da sie einen wichtigen Teilaspekt des in Abs. 1 übergreifend geregelten Datenschutzes durch Gestaltung spezifiziert (Lang 2019). Die Voreinstellung ist dabei die standardgemäße Einstellung, die der Dienstanbieter im Nutzungsprofil einem Anwender anbietet. Die Verordnung stellt nun sicher, dass nicht der Anwender selbst die unnötige Datenerhebung abstellen, sondern sie von Dienstanbieter proaktiv eingestellt werden muss; damit reagiert der Gesetzgeber auf die Neigung der meisten Menschen, Voreinstellungen zu akzeptieren (sog. status quo bias) und verhindert, dass diese psychologische Prädisposition ausgenutzt wird (Schantz und Wollf 2017). Dabei überlässt die Vorschrift dem Betreiber nicht die alleinige Gestaltungsfreiheit, sondern stellt sie in den Dienst des Schutzes der privaten Interessen: Sie dürfen nicht ausschließlich den wirtschaftlichen Zielsetzungen des Diensteanbieters bzw. Verantwortlichen im Sinne einer Maximierung von Datenströmen verschrieben sein, sondern müssen vielmehr dem Gebot der Erforderlichkeit für die Zweckerfüllung genügen (Martini 2018). Anwender, die ein Informations- und Kommunikationssystem verwenden, welches das Privacy-by-Default-Konzept beachtet, können daher davon ausgehen, dass die Systeme bei der erstmaligen Verwendung grundsätzlich datenschutzrechtskonform sind. Durch eine Änderung der Werkseinstellungen können allerdings spezifische Daten freigegeben werden (Kipker 2015).

6.3 Erste Bewertung der gesetzlichen Regelung

Die Konzepte des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen gehören zu den Kernelementen und Innovationsträgern der DSGVO; beide Datenschutzkonzepte sind von dem Ziel getragen, der Komplexität moderner Datenverarbeitungsvorgänge auf einer möglichst niedrigschwelligen Ebene zu begegnen und dem Verantwortlichen technische Spezifikationen als Grundmodus abzuverlangen, die durch Datenminimierung und Zweckbindung für ein entsprechendes Datenschutzniveau sorgen (Martini 2018). Trotz dieser Zielrichtung wird nur der Verantwortliche in die Pflicht genommen, obwohl nahegelegene hätte, auch Vorgaben für Hersteller von Produkten, Diensten, Anwendungen und Geräten festzulegen (Schantz und Wollf 2017). Nach Erwägungsgrund 78 Satz 4 DSGVO sollten die Hersteller lediglich ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung zu berücksichtigen. Sie sollen unter gebührender Berücksichtigung des Stands der Technik sicherstellen, dass die Verantwortlichen in der Lage sind, ihren Datenschutzpflichten nachzukommen. Da aber der Anwender verpflichtet wird, diejenige Technik auszuwählen, die den Da-

tenschutz gewährleistet, werden die Angebote der Hersteller mittelbar doch beeinflusst (Rose 2017).

6.4 Anwendungsbereich bei Smart-Glasses-basierten Applikationen

Besonders bei Smart-Glasses-basierten Anwendungen ist eine datenschutzrechtliche Berücksichtigung nach dem Privacy-by-Design-Ansatz notwendig. Schwenke (2015, 2018) benennt die wesentlichen rechtlichen Probleme von Smart Glasses im öffentlichen Raum. Zum einen werden Abbildungen und Stimmen Dritter durch die an Smart Glasses montierte Kamera und dem Einsatz einer sprachbasierten Steuerung, ggf. ohne deren Kenntnis, erfasst. Damit ist die Möglichkeit gegeben, sensible Informationen unbemerkt von Dritten aufzuzeichnen und den Schutz der Privatsphäre zu verletzen. Aufgrund der geringen Rechenkapazität von Smart Glasses ist davon auszugehen, dass diese Informationen an Dritte, genauer: an Cloud-Dienstleister, weitergegeben werden, wodurch der Kontrollverlust der erhobenen Daten und eine fehlende Abschätzung, inwiefern die Daten weiterverarbeitet werden, zunehmen.

6.5 Nutzungskonzepte einzelner Smart-Glasses-Modelle

Bei der Gestaltung von Smart-Glasses-basierten Anwendungen kann das Privacy-by-Design-Konzept im Rahmen der Technologieauswahl und der softwaretechnischen Umsetzung realisiert bzw. beachtet werden. Beispielsweise ermöglichen die Smart-Glasses-Modelle der Vuzix Blade sowie der HMT-1 von Realwear eine lokale sprachbasierte Erkennung, sodass keine Informationsverarbeitung der Audioaufnahmen bei einem Cloud-Dienstleister erfolgt. Eine verbaute Privacy-LED leuchtet bspw. bei der Vuzix M300 rot, wenn der Smart-Glasses-Anwender die Kamera aktiviert, dadurch werden unbemerkte Bild- und Videoaufnahmen erschwert.

Für die softwaretechnische Realisierung entwickelten Diamantopoulou et al. (2017) Privacy-by-Design-Patterns und -Maßnahmen, die konkrete Empfehlungen bei der softwaretechnischen Verarbeitung und Verbreitung von Informationen liefern. Dabei berücksichtigen die Patterns insb. die folgenden fünf Datenschutzvorgaben: Anonymität, Pseudonymität, Nichtverkettbarkeit, Undeutlichkeit sowie Unbeobachtbarkeit.

6.6 Mögliche Datenschutzverletzungen im Verarbeitungsprozess

Die vier verschiedenen Datenverarbeitungsschritte Informationserfassung, Informationsverarbeitung, Informationsverbreitung und Beeinflussung wurden von Solove (2006) als die möglichen Aktivitäten einer Datenschutzverletzung identifiziert (vgl. [Abb. 8](#)). Mit den einzelnen Datenverarbeitungsschritten geht für den

Anwender ein zunehmender Verlust an Kontrolle über die erfassten Informationen, wie Bild-, Video- und Audioaufnahmen, einher. Dabei findet keine klare Trennung zwischen den Informationen des Datensubjektes und externen Dritten statt. Diese Daten werden im Rahmen sog. Cloud-Services weiterverarbeitet, bspw. analysiert ein Service zur Spracherkennung die zur Cloud gesendeten Audioaufnahmen und gibt die erkannten Ergebnisse an den Benutzer weiter. Der Anwender hat nur ein bedingtes Wissen, inwiefern der Cloud-Dienstleister diese Daten an Dritte weitergibt. Der Kontrollverlust über erfasste Informationen nimmt zu. Beeinflussungen können insofern auftreten, dass der Anwender basierend auf den erhobenen, ausgewerteten und freigegebenen Informationen z.B. von Externen abgestimmte Informationen erhält.

Abb. 8. Datenverarbeitungsschritte und mögliche Aktivitäten der Datenschutzverletzung bei der Verwendung von Smart Glasses, angelehnt an Solove (2006) und Schwenke (2015, 2018)

Die Abbildung verdeutlicht, dass ungenügende Maßnahmen für einen effektiven Datenschutz und die Sicherheit der Daten bereits nach der Erfassung der Daten ungewollte und nicht kontrollierbare Effekte zur Folge haben können.

6.7 Privacy-by-Design in der praktischen Umsetzung

Das Risiko möglicher Datenschutzverletzungen bei der Anwendung von Smart Glasses zwingt dazu, die Regelungen der DSGVO in der praktischen Umsetzung zu beachten. Im Ergebnis ist festzuhalten, dass die DSGVO den gesetzgeberischen Auftrag zur Verwirklichung eines effektiven Datenschutzes nur sehr abstrakt umsetzt und insb. Art und Umfang von Sicherungsmaßnahmen dem Verantwortlichen

überlässt. Kann dieser nicht sicher beurteilen, ob er dem geforderten Datenschutz in angemessener Weise Rechnung trägt, führt die verbleibende Rechtsunsicherheit zu einem Risiko für den Anwender.

Im Anwendungsbereich von Smart-Glasses-basierten Applikationen, die auf die Verarbeitung von personenbezogenen Daten ausgerichtet sind, sind die Vorgaben der DSGVO zu beachten. In der Umsetzung können zum gegenwärtigen Zeitpunkt jedoch keine verlässlichen Nutzungskonzepte präsentiert werden. So hat der Europäische Datenschutzbeauftragte im Januar 2019 zwar seinen ersten Technologie-report mit dem Titel „Smart Glasses and Data Protection“ veröffentlicht, sich darin aber nur auf sehr allgemeine Aussagen zu den Datenschutzprinzipien und den Rechten der von der Datenverarbeitung Betroffenen beschränkt; statt dessen wurde auf Entscheidungen zu anderen Technologien, wie etwa Dash-Cams, CCTV oder Gesichtserkennungssystemen, verwiesen (Hänold 2019). Vor diesem Hintergrund ist nicht zeitnah damit zu rechnen, dass der Europäische Datenschutzausschuss oder andere Datenschutzbehörden entsprechende Leitlinien, Verhaltensregeln oder Zertifizierungsschemata veröffentlichen werden (Hänold 2019). Es sind also unmittelbar der Techniknutzer als Verantwortlicher im Sinne der DSGVO und mittelbar der Hersteller berufen, den Datenschutz durch Einsatz der Konzepte von Privacy-by-Design und Privacy-by-Default in ihrem Rahmen bestmöglich zu realisieren.

6.8 Privacy-by-Design außerhalb des Datenschutzes

Der Ansatz von Privacy-by-Design-and-by-Default wirkt sich jedoch nicht nur in datenschutzrechtlicher Sicht aus. Er zeitigt auch Ausstrahlungswirkung in Bereichen, die außerhalb des eigentlichen Datenschutzes liegen, und wird umgekehrt auch von solchen beeinflusst.

Ein zu beachtender Blickwinkel ist die *soziotechnische Sicht auf die Technikgestaltung* durch Verwirklichung eines sog. „*Partizipativen Privacy-by-Design*“ (Ochs et al. 2016). Ansatzpunkt ist die Verbindung der Ansätze des Privacy-by-Design und des Participatory-Design zur Schaffung eines „Third Space“, in dem sich Technik-Entwickler und Anwender auf Augenhöhe begegnen und den Entwicklungsprozess kooperativ betreiben (Ochs et al. 2016). Hintergrund dieses Ansatzes ist die Erkenntnis, dass durch die fortschreitende Digitalisierung immer weiterer Lebensbereiche auch die Eingriffsintensität in die (Grund)Rechte der betroffenen Personen zunimmt. Wie gezeigt werden im Datenschutzrecht Risiken für die Beeinträchtigung von (Grund)Rechten der von der Datenverarbeitung betroffenen Personen durch Regelungen adressiert. Sie regulieren die Beschaffenheit von technischen Systemen und organisatorischen Prozessen, in die diese eingebettet sind, treffen aber gerade keine Regelungen für Hersteller (Ochs et al. 2016). Die vielfältigen Konflikte, die sich gegenwärtig an den Prozessen der Digitalvernetzung entzünden und diskursiv artikuliert werden, scheinen die Notwendigkeit der Frage nach der demokratischen Partizipation an der Gestaltung der Technologien zu bestätigen (Ochs et al. 2016). Dabei ist zu beachten, dass die fortschrei-

tende Digitalisierung der Gesellschaft und der Umgang mit Daten und Wissen politisch determiniert sind und daher einer demokratischen Legitimation im Sinne einer Teilhabe der betroffenen und beteiligten Personen bedürfen. Ein gesellschaftliches Problem kann nicht allein durch Technikgestaltung gelöst werden.

Als Vorbild für eine effektive Umsetzung eines gesetzlichen Auftrages ist das *Technikrecht im Arbeitsschutz* zu nennen, welches seit mehr als zwei Jahrzehnten den Schutz des Verwenders durch stetige Modernisierung des Regulierungsregimes verbessert. Hierzu dient ein System aus verbindlichen Verordnungen und technischen Regeln (etwa Arbeitsstättenverordnung, Gefahrstoffverordnung, Betriebssicherheitsverordnung). Diese häufig aktualisierten Vorgaben beschreiben praxisnah und anschaulich, durch welche organisatorischen und technischen Maßnahmen die allgemeinen Anforderungen der Arbeitsschutzverordnungen erfüllt werden können. Dieser hohe Konkretisierungs- und Verbindlichkeitsgrad der technischen Regeln im Arbeitsschutz sowie die effektive Besetzung der die Regeln schaffenden Arbeitsschutzausschüsse könnten als Vorbild auch für das Datenschutzrecht dienen (Rose 2017).

Nicht zu vernachlässigen ist ferner die *wirtschaftliche Sicht bei Verfolgung des Privacy-by-Design-Ansatzes durch Hersteller*. Wenngleich Hersteller von Smart Glasses – oder sonstigen Gegenständen des Internet of Things (IoT) – nicht Adressaten des Datenschutzes sind, so besteht doch ein enormer Wettbewerbsvorteil, wenn die Geräte technisch in der Lage sind, den Datenschutz zu erfüllen, zu dessen Beachtung der jeweilige Anwender/Dienstleister gesetzlich verpflichtet ist. Er ist davon auszugehen, dass sich ein Anwender im Zweifel für ein datenschutzfreundliches Produkt entscheiden wird. Andererseits kann diese Sichtweise aber auch dazu führen, dass der wissenschaftliche Fortschritt in Forschung und Entwicklung gehemmt wird, weil Neuerungen nicht immer datenschutzfreundlich sind und somit möglicherweise nicht weiterverfolgt werden.

Abschließend soll auch auf die *finanzielle Sicht des Anwenders* als dem gesetzlich Verantwortlichen hingewiesen werden, der *bei Datenschutzverstößen mit staatlichen Sanktionen zu rechnen hat*. Die DSGVO normiert ein umfassendes System von Sanktionen, wozu im weiteren Sinne die Garantie der Klagemöglichkeiten bei Verletzung von Datenschutzbestimmungen und die Haftungsregelungen in Form von Schadensersatzansprüchen sowie die Sanktionen im engeren Sinne, d.h. die Ordnungswidrigkeiten und die Strafnormen, zählen (Schantz und Wolff 2017). So können etwa nach Art. 83 Abs. 5 DSGVO drastische Datenschutzverstöße mit Geldbußen von bis zu 20 Mio. € oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher der Beträge höher ist, geahndet werden. Vor diesem Hintergrund wird jedem Anwender daran gelegen sein, die Vorgaben des Datenschutzes bestmöglich zu erfüllen, um solche Sanktionen zu vermeiden. Allerdings besteht dadurch auch die Gefahr, dass Anwender den Datenschutz in den Vordergrund stellen und somit die eigentlichen Nutzungsmöglichkeiten von Smart Devices nicht ausschöpfen.

7 Fazit und Ausblick

Durch die Kombination der Methoden KORA, Experteninterviews und Literaturrecherche im Rahmen des DSR-Ansatzes Heuristic Theorizing wurde ein Datenschutz-Framework für Smart-Glasses-basierte Informationssysteme in der Logistik entwickelt. Es kann eine Ergänzung um domänenspezifische Anforderungen für weitere Branchen erfolgen in dem das Framework und das methodische Vorgehen als Basis für weitere Forschungsarbeiten herangezogen werden.

Das Framework ergänzt vorhandene Datenschutzregelungen um Anforderungen aus der Informationsprivatheit durch die Integration verschiedener Stakeholder-Perspektiven. Um die Forschungslücke der Integration der Anwender in Gestaltung und Evaluation entsprechender Systeme weiter zu schließen, ist das Framework mittels einer Instanziierung durch einen Prototyp zu untersuchen. In diesem Zusammenhang ergibt sich die weiterführende Fragestellung (F3) *Wie können Maßnahmen der Informationsprivatheit in der Systementwicklung umgesetzt werden?* Dazu werden zunächst einzelne Lösungskomponenten weiter spezifiziert, insb. die mit der DSGVO rechtlich verankerten Grundsätze der Systementwicklung Privacy-by-Design und Privacy-by-Default. Somit ergibt sich u.a. als fortführende Forschungsfrage (F3.1) *Wie können auf dem aktuellen Stand der Datensicherheit, die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO für Smart Glasses im betrieblichen Einsatz gestaltet und kontrolliert werden?* Darüber hinaus sind insb. Privacy-Enhancing-Technologies im Sinne des Art. 25 DSGVO, zur Umsetzung des Selbstdatenschutzes in einer vom Internet of Things geprägten Arbeitswelt zu konkretisieren. Die Ergebnisse dieser Ausarbeitung dienen darüber hinaus als Basis für weitere Forschung im Bereich Informationsprivatheit als Einflussgröße der Technologieakzeptanz, um die Anwenderperspektive nachhaltig in den Fokus der datenschutzrechtlichen Gestaltung von Informationssystemen zu rücken.

In dem vorliegenden Beitrag wird die Wissensbasis im Bereich der Informationsprivatheit erweitert durch ein Framework zur datenschutzrechtlich konformen Gestaltung von Smart-Glasses-basierten Informationssystemen, sowie ein praxisrelevanter Beitrag geleistet durch die Ableitung entsprechender Design-Prinzipien. Aktuell wird das vorgestellte Framework von den Autoren genutzt, um ein Smart-Glasses-basiertes Informationssystem zur Unterstützung von Logistikdienstleistern zu implementieren. Dabei unterstützt das Framework als Diskussionsgrundlage zur gemeinsamen Konzeption mit einem mittelständischen und einem großen Unternehmen der Logistik.

8 Literatur

Baumgartner U (2018) Art. 25 DS-GVO. In: Ehmann E, Selmayr M (Hrsg) Datenschutz-Grundverordnung. C.H. Beck, München, 2. Auflage

- Bélanger F, Crossler RE (2011) Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly* 35(4):1017–1041
- Bechtle und SAP (2016) Smarte Brillen optimieren Lagerlogistik. In: *it&t business* Bd. 02–03/2016, 27–28
- Bizer J, Dingel K, Fabian B, Günther O, Hansen M, Klaffit M, Möller J, Spiekermann S (2006) Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS). Fraunhofer-Publica, <http://publica.fraunhofer.de/dokumente/N-51890.html>, abgerufen am 07.07.2020
- Gregory RW, Muntermann J (2014): Generating Design Theories Heuristic Theorizing: Proactively Generating Design Theories. *Information Systems Research* 25(3):639–653
- Hackenberg W (2019) Big Data und Datenschutz In: Hoeren T, Sieber U, Holznapel B (Hrsg) *Multimedia-Recht*. C.H. Beck, München
- Hammer V, Pordesch U, Roßnagel A, Zeidler G (1993) Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet. Springer, Berlin Heidelberg
- Hänold S (2019) EDSB: Smart Glasses – erster Technologiereport. *Zeitschrift für Datenschutz* 7(2019)
- Hartung J (2018) Art. 25 DS-GVO. In: Kühling J, Buchner B (Hrsg) *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO/BDSG*. C.H. Beck, München, 2. Auflage
- Hevner AR, March ST, Park J, Ram S (2004) Design Science in Information Systems Research. *MIS Quarterly* 28(1):75–105
- Kipker D-K (2015) Privacy by Default und Privacy by Design. *Datenschutz und Datensicherheit* 39(6):410
- Martini M (2018) Art. 25 DS-GVO. In: Paal BP, Pauly DA (Hrsg) *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*. C.H. Beck, München, 2. Auflage
- Niemöller C, Metzger D, Fellmann M, Özcan D, Thomas O (2016) Shaping the Future of Mobile Service Support Systems – Ex-Ante Evaluation of Smart Glasses in Technical Customer Service Processes. In: Mayr HC, Pinzger M (Hrsg) *Informatik 2016*. Gesellschaft für Informatik e.V., Bonn, 753–767
- Nohl AM (2012) Interview und dokumentarische Methode. Springer, Wiesbaden, 4. Auflage
- Ochs C, Richter P, Uhlmann M (2016) Technikgestaltung demokratisieren – Partizipatives Privacy by Design. *Zeitschrift für Datenschutz* 6(2016)
- Paal BP, Pauly DA, Ernst S; Frenzel EM, Körffler B, Matini M. (2017) *Datenschutz-Grundverordnung, Beck'sche Kompakt-Kommentare*
- Pavlou PA (2011) State of the Information privacy Literature: Where Are We and Where Should We Go? *MIS Quarterly* 35(4):977–988
- Rose E (2017) Smart Cams im öffentlichen Raum. *Zeitschrift für Datenschutz* 2(2017):64–68
- Roßnagel A (2007) *Datenschutz in einem informatisierten Alltag*. Friedrich Ebert Stiftung, Berlin
- Schantz P, Wolff HA (2017) *Das neue Datenschutzrecht*. C.H. Beck, München
- Schwenke T (2015) Schnittstellen zum „Cyborgspace“ – Erkenntnisse zu Datenbrillen nach Ende des „Google Glass“-Experiments. *Datenschutz und Datensicherheit* 39:161–166. doi: 10.1007/s11623-015-0386-8
- Schwenke T (2018) Rechtsprobleme der Nutzung von Smart Glasses und Smart Lenses im öffentlichen Raum. In Albers M, Katsivelas I (Hrsg) *Recht & Netz, Nomos*, 469–490

- Schulz T, Skistims H, Zirfas J, Comes D, Evers C (2011) Vorschläge zur rechtskonformen Gestaltung selbst-adaptiver Anwendungen. In: Heiß HU, Pepper P, Schlinghoff H, Schneider H (Hrsg) Informatik 2011. Gesellschaft für Informatik e.V., Berlin, 182–184
- Solove, Daniel J (2006) A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154 (3):477–564
- Thomas O, Nüttgens M, Fellmann M, Krumeich J, Hücke S, Breitschwerdt R, Rosenkranz N, Schlicker M, et al. (2014) Empower Mobile Technical Customer Services (EMO-TEC). In: Nüttgens M, Thomas O, Fellmann M (Hrsg) Dienstleistungsproduktivität. Springer Fachmedien, Wiesbaden
- Thüsing G, Forst G, Granetzny T, Pötters S, Traut J (2014) Beschäftigtendatenschutz und Compliance: Effektive Compliance im Spannungsfeld von BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung. C.H. Beck, München, 2. Auflage
- van Rest J, Boonstra D, Everts M, van Rijn M, van Paassen R (2014) Designing Privacy-by-Design. In: Preneel B, Ikonomou D (Eds) *Privacy Technologies and Policy*. Springer Berlin Heidelberg, 55–72
- Wächter M (2003) *Datenschutz im Unternehmen*. C.H. Beck, München, 4. Auflage