Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 1037

Datenschutzrechtliche Anforderungen an Smart Glasses-basierende Informationssysteme in der Logistik

Lisa Berkemeier[1], Mary-Rose McGuire[2], Sabrina Steinmann[2], Christina Niemöller[1] und Oliver Thomas[1]

Abstract: 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. Insbesondere 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 Gestaltungsvorschlägen für Smart Glasses-basierende 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.

Keywords: Datenschutz, Informationsprivatheit, BDSG, DSGVO, Smart Glasses, KORA, Logistik

1 Einleitung

Forschungen im Bereich Service Science haben mobile Informationssysteme als notwendiges Instrument zur Bewältigung der vielfältigen Aufgaben im Dienstleistungssektor identifiziert [TNFK14]. Insbesondere Smart Glasses-basierende Informationssysteme sind zur Unterstützung von informationsintensiven Prozessen geeignet [NMFÖ16]. 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

[1] Universität Osnabrück, Informationsmanagement und Wirtschaftsinformatik, Katharinenstr. 3, 49074 Osnabrück, vorname.nachname@uni-osnabrueck.de
[2] Universität Osnabrück, Lehrstuhl für Bürgerliches Recht, Recht des Geistigen Eigentums sowie deutsches und europäisches Zivilprozessrecht, Katharinenstr. 15, 49074 Osnabrück, vorname.nachname@uni-osnabrueck.de

doi:10.18420/in2017_106

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 – ab Mai 2018 anwendbar. Gemeinsamer Nenner all dieser Rechtsgrundlagen ist, dass sie die Datensouveränität 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-basierenden Systemen, berücksichtigen jedoch nicht explizit Anforderungen an einen umfassenden Datenschutz [NMFÖ16]. 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 [BeSa16] wurde diese als Anwendungsdomäne fokussiert. Die Erkenntnisse zu den Anforderungen an den Datenschutz von Smart Glasses-basierenden Informationssystemen 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-basierenden 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 Ergebnisse zusammengefasst und weiterer Forschungsbedarf aufgezeigt.

2 Stand der Wissenschaft

Der Funktionsumfang aktueller Smart-Glasses-Modelle erfasst und nutzt Daten über den Nutzer 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 Nutzers erfasst [NMFÖ16]. Smart Glasses

sind auf Grund dieser Eingriffe in die Privatsphäre, sowohl des Nutzers, 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 [BéCr11]. Unter Berücksichtigung dieser Kritik ist die Integration potenzieller Anwender und konkreter Anforderungen des Datenschutzes ein essentieller Faktor, bereits im Design und der Implementierung eines Smart Glasses-basierenden 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 [Wäch03]. 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 [Schw15]. 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 [BéCr11].

3 Forschungsstrategie zur Entwicklung eines Smart Glasses-basierenden 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 Nutzer, folgt die Forschungsstrategie einem iterativen Design Science Research-Ansatz (DSR). In der klassischen DSR werden Meta-Anforderungen und Lösungskomponenten definiert und iterativ evaluiert. [HMPR04] 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 [GrMu14] (vgl.Abb. 1). Für die Systemkonzeption werden Meta-Anforderungen sowohl aus den juristischen Anforderungen, insbesondere der DSGVO, als auch der wirtschaftswissenschaftlichen Literatur hergeleitet und durch spezifische Anforderungen der befragten Nutzer 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 3.2). Für die Entwicklung der Meta-Anforderungen und Lösungskomponenten haben einzelne Methoden zur Identifikation relevanter Literatur (vgl. Abschnitt 2) und der Befragung von Experten (vgl. Abschnitt 3.3), Informationen generiert.

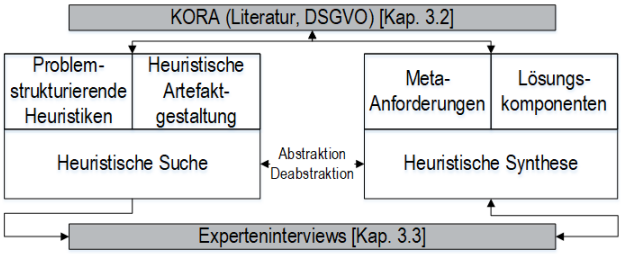

Abb. 1: Methodisches Vorgehen

Konkretisierung rechtlicher Anforderungen. Die Identifikation der relevanten rechtlichen Anforderungen sowie die sich daraus ergebenden Vorgaben an das Smart Glasses-basierende 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 [SSZC11]. 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 [HaPR93]. Hinzuweisen ist darauf, dass sich das Ziel dieses Beitrags auf die Konkretisierung der datenschutzrechtlichen Anforderungen an Smart Glasses-basierende 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.

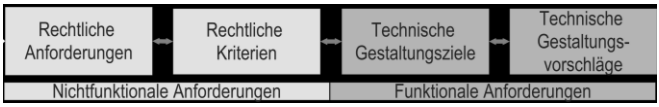

Abb. 2: Konkretisierung rechtlicher Anforderungen

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 Nutzer des Informationssystems sind insbesondere 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 invasiver Technologien ableiten. So wurden die Exper-

ten 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) [Nohl12].

4 Ableitung datenschutzrechtlicher Anforderungen an Smart Glasses-basierende Informationssysteme

4.1 Rechtliche Anforderungen

Vornehmlich konkretisiert die DSGVO die rechtskonforme automatisierte Datenverarbeitung, genauer die Erhebung, Verarbeitung und Nutzung, von personenbezogenen Daten [PaPa17]. 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 [PaPa17]. 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 Mitgliedstaaten 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 „persönlichen 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 basierenden 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 mindestens von zwei verschiedenen Autoren genannt und stehen in einer interdependenten Beziehung zueinander.

Konstrukte aus der Literatur	Ausprägungen der Konstrukte								
[BDFG14]	Rechts-durchsetzung	Zweck-bindung	Transparenz	Rechtliche Rahmen-bedingungen technischer Schutz-mechanismen	k.A.	k.A.	Datensparsame Technik-gestaltung	k.A.	Inter-nationalität & Outsourcing / Verantwortlich-keiten
[Thüs14]	Einwilligung	Zweck-bindungs-grundsatz	Rechte auf Auskunft	k.A.	k.A.	k.A.	Datenvermeidung und -Sparsamkeit	Mitbestim-mungs-recht	k.A.
[Bize07]	Rechtmäßigkeit / wirksame Einwilligung	Zweck-bindung	Transparenz	Datensicherheit	Erforder-lichkeit	Kontrolle	k.A.	k.A.	k.A.
[HaPR93]	Entscheidungs-freiheit	Zweck-bindung	Transparenz	Techniksicherung	Erforder-lichkeit	Kontroll-eignung	k.A.	Anpassung s-fähigkeit	Arbeits-erleichterung / Werkzeug-eignung
[Roßn07]	Besondere Zulassung	Zweck-bindung	Transparenz	Selbst- und System-datenschutz	Erforder-lichkeit	Kontrolle	k.A.	Mitwirkung	k.A.
Rechtliche Kriterien	**Einwilligung**	**Zweck-bindung**	**Transparenz**	**Datensicherheit**	**Erforder-lichkeit**	**Kon-trolle**	**Daten-vermeidung und -sparsamkeit**	**Mit-wirkung**	keine Zuordnung

Abb. 3: Herleitung der rechtlichen Kriterien aus der Literatur

4.3 Ziele technischer Gestaltung

Die Ziele der technischen Gestaltung eines Smart Glasses-basierenden 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 insgesamt 16 Meta-Anforderungen an die Lösungskomponenten des Datenschutzes von Smart Glasses-basierenden Informationssystemen identifiziert. Aus der DSGVO können sowohl direkte als auch implizite Anforderungen an die Gestaltung eines Smart Glasses-basierenden 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 [PaPa17]. Eine Übersicht wird in Abb. 5 dargestellt.

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			(MA10) Mitarbeiter von vornherein einbeziehen
Mitarbeiter vorab einbeziehen	x	x		
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 (Abschnitt 4.4) und konkreten Lösungselementen aus der Literatur. Insbesondere 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 Mindestmaß-

nahmenkatalog spezifiziert werden [PaPa17]. 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.

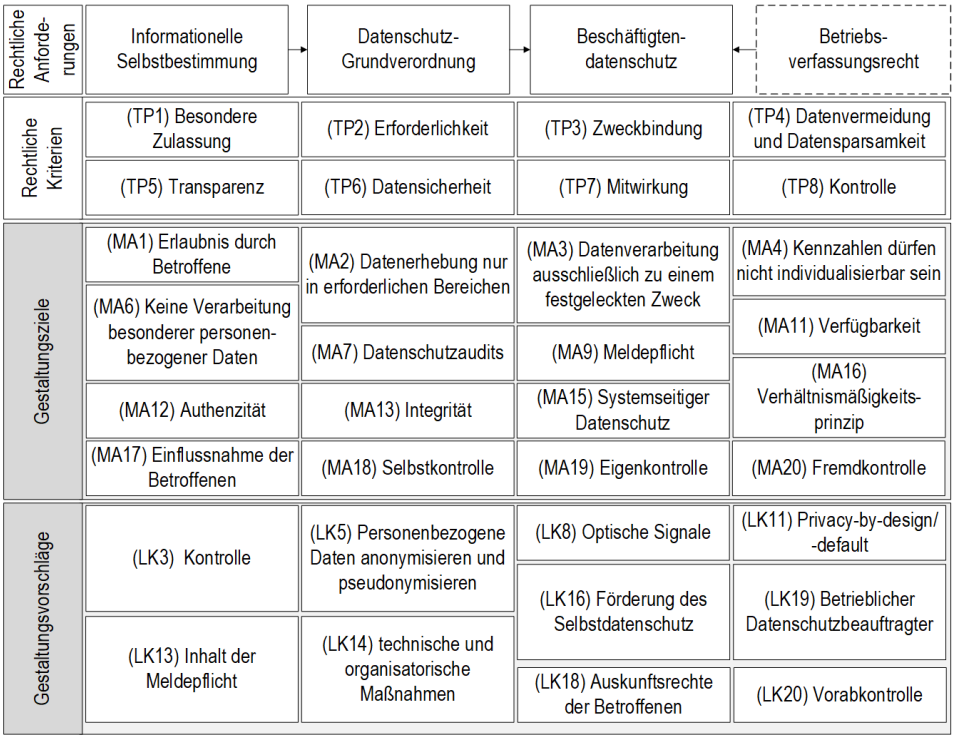

Abb. 5: Ergebnisse der KORA, basierend auf der Literatur

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-basierenden 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-basierenden 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
TP5	Transparenz	MA7	Datenschutzaudits	LK10	Sicherheitsstandards
		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	LK10	Sicherheitsstandards

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

Passieren Smart-Glasses-Nutzer 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 [Pavl11] und erweitern die Möglich-

keiten des Selbstdatenschutzes der Anwender durch die Nutzung entsprechender Technologien.

6 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-basierende 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, insbesondere 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 insbesondere 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 Nutzerperspektive nachhaltig in den Fokus der datenschutzrechtlichen Gestaltung von Informationssystemen zu rücken. In dem vorliegenden Paper wird die Wissensbasis im Bereich der Informationsprivatheit erweitert durch ein Framework zur datenschutzrechtlich-konformen Gestaltung von Smart Glasses-basierenden 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.

Danksagung

Dieser Beitrag ist Teil des Projekts Glasshouse, welches vom Bundesministerium für Bildung und Forschung (BMBF) unter dem FKZ. 01FJ15062 gefördert wird.

Literaturverzeichnis

[BéCr11] Bélanger, France und Crossler, Robert E: Privacy in the digital age: A review of information privacy research in information systems. In: *MIS Quarterly* Bd. 35 (2011), Nr. 4, S. 1017–1041

[BeSa16] Bechtle ; SAP: Smarte Brillen optimieren Lagerlogistik. In: *it&t business* Bd. 02–03/2016 (2016), S. 27–28 — ISBN 2081066066481

[GrMu14] Gregory, Robert Wayne und Muntermann, Jan: Generating Design Theories Heuristic Theorizing : Proactively Generating Design Theories. In: *Information Systems Research* Bd. 25 (2014), Nr. 3, S. 639–653 — ISBN 10477047

[HaPR93] Hammer, Volker ; Pordesch, Ulrich ; Roßnagel, Alexander und Gerhard Zeidler (Hrsg.): *Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet* : Springer Berlin Heidelberg, 1993 — ISBN 9783540565116

[HMPR04] Hevner, Alan R ; March, Salvatore T ; Park, Jinsoo und Ram, Sudha: Design Science in Information Systems Research. In: *MIS Quarterly* Bd. 28 (2004), Nr. 1, S. 75–105

[NMFÖ16] Niemöller, Christina ; Metzger, Dirk ; Fellmann, Michael ; Özcan, Deniz und Thomas, Oliver: Shaping the Future of Mobile Service Support Systems – Ex-Ante Evaluation of Smart Glasses in Technical Customer Service Processes. In: *Informatik 2016*. Klagenfurt, 2016

[Nohl12] Nohl, Arnd-Michael: *Interview und dokumentarische Methode*. 4. Auflage. Aufl. Wiesbaden : Springer VS, 2012 — ISBN 978-3-486-71955-0

[PaPa17] Paal, Boris P. ; Pauly, Daniel A. ; Paal, B. P. ; Pauly, D. A. ; Ernst, S. ; Frenzel, E. M. ; Körffer, B. und Matini, M. (Hrsg.): *Datenschutz-Grundverordnung* : Beck'sche Kompakt-Kommentare, 2017

[Pavl11] Pavlou, Paul A: State of the Information privacy Literature: Where Are We and Where Should We Go? In: *MIS Quarterly* Bd. 35 (2011), Nr. 4, S. 977–988

[Schw15] Schwenke, Thomas: Schnittstellen zum „ Cyborgspace " – Erkenntnisse zu Datenbrillen nach Ende des „ Google Glass " -Experiments Warum das Konzept der Privatsphäre in einer. In: *DuD* Bd. 3 (2015)

[SSZC11] Schulz, Thomas ; Skistims, Hendrik ; Zirfas, Julia ; Comes, Diana und Evers, Christoph: Vorschläge zur rechtskonformen Gestaltung selbst-adaptiver Anwendungen. In: *Informatik*. Berlin, 2011 — ISBN 9783885792864, S. 182–184

[TNFK14] Thomas, O ; Nüttgens, M ; Fellmann, M ; Krumeich, J ; Hucke, S ; Breitschwerdt, R ; Rosenkranz, N und Schlicker, M ; U. A.: Empower Mobile Technical Customer Services (EMOTEC) – Produktivitätssteigerung durch intelligente mobile Assistenzsysteme im Technischen Kundendienst. In: NÜTTGENS, M. ; THOMAS, O. ; FELLMANN, M. (Hrsg.): *Dienstleistungsproduktivität* : Springer Fachmedien Wiesbaden, 2014. — NULL, S. 2–17

[Wäch03] Wächter, Michael: *Datenschutz im Unternehmen*. 4. Aufl. München : CH Beck, 2003 — ISBN 3406492533