FORUM Wirtschaftsrecht - Band 21

Institut für Wirtschaftsrecht

Carolin Hohmann

Datenschutz bei Wearable Computing

Eine juristische Analyse am Beispiel von Google Glass

kassel university press

FORUM Wirtschaftsrecht

Band 21

Herausgegeben vom
Institut für Wirtschaftsrecht an der Universität Kassel

Datenschutz bei Wearable Computing

Eine juristische Analyse am Beispiel von Google Glass

Carolin Hohmann

kassel university press

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar

ISBN: 978-3-7376-0082-8 (print)
ISBN: 978-3-7376-0083-5 (e-book)
URN: http://nbn-resolving.de/urn:nbn:de:0002-400837

www.uni-kassel.de/upress

Printed in Germany

Vorwort der Herausgeber

Das selbstgewählte Thema greift ein sehr aktuelles und zukunftsweisendes Rechtsproblem auf, nämlich die datenschutzrechtliche Bewertung von Wearable-Computing-Anwendungen. Diese sind Teil des großen Trends hin zu einer Informatisierung des Alltags. Immer mehr Alltagsgegenstände werden mit Sensor-, Kommunikations- und Rechnertechnik ausgestattet. Dadurch findet Datenverarbeitung zwar allgegenwärtig, aber im Hintergrund statt. Der Mensch hat nicht mehr nur ein einziges für die Datenverarbeitung bestimmtes Gerät (Computer), vielmehr wird seine gesamte Umgebung mit der Kapazität zur Datenverarbeitung und zur Kommunikation ausgestattet. Die ihn umgebenden Dinge können durch Sensoren ihre Umgebung wahrnehmen. Jedem Ding ist eine Webseite zugeordnet, auf der diese Informationen gespeichert und abgerufen werden können. Im Internet der Dinge erhalten die Gegenstände ein „Gedächtnis" und können ihre Informationen (Nutzungsgeschichte, Gebrauchsanweisung, Reparaturanleitung und ähnliche Informationen) dem Nutzer mitteilen.

Trägt der Mensch diese „intelligenten" Dinge am Körper, spricht man von „Wearable Computing". Uhren, Schmuck, Kleidung und (Fitness-) Armbänder erfassen Körperfunktionen ihres Trägers, nehmen über Sensoren, Mikrofone oder Minikameras Veränderungen in ihrer Umgebung wahr und bestimmen über Ortungsgeräte ihren jeweiligen Aufenthaltsort. Die so gewonnenen Daten können sie aufgrund eines Modells ihrer Umwelt einordnen und bewerten. Sie sind daher in der Lage, ihrem Nutzer quasi „mitdenkend" kontextbezogen umfangreiche Zusatz- und Hintergrundinformationen anzubieten. Die Kommunikation zwischen Mensch und Gegenstand erfolgt durch der Situation angepasste Eingabemedien wie Sprach-, Handschrift- und Bilderkennung sowie durch Ausgabemedien wie Sprache, Projektionen auf Wände oder die Netzhaut oder leuchtfähiges Plastik.

Wird der Mensch durch die Datenverarbeitung an oder in seinem Körper allgegenwärtig begleitet, wird diese unmerklich Teil seines

Verhaltens und seines Handelns. Die exponentielle Zunahme von personenbezogenen Daten mit hoher Aussagekraft erlaubt, individuelles Verhalten ebenso detailliert nachzuvollziehen wie kollektive Lebensstrukturen und beide zu beeinflussen. Die Individualisierung der Unterstützung zwingt zu detaillierten Profilen mit Angaben zu Verhaltensweisen, Beziehungen, Einstellungen und Vorlieben. Diese Entwicklung eröffnet bisher unbekannte Potenziale und Risiken gesellschaftlicher Kontrolle und individueller Fremdsteuerung.

Das bisher leistungsfähigste und prominenteste Beispiel für Wearable Computing ist die Datenbrille von Google. Auch wenn „Google Glass" inzwischen erst einmal wieder zurückgezogen wurde, ist sie geeignet, Chancen und Risiken zu erkennen und zu bewerten. Gerade wenn die Brille überarbeitet und dann neu angeboten werden soll, ist sie das ideale Objekt für die Frage, ob und wie Wearable Computing datenschutzgerecht gestaltet werden kann.

Diese Frage hat Frau Hohmann in ihrer Masterarbeit „Datenschutz bei Wearable Computing – Eine juristische Analyse am Beispiel von Google Glass" aufgenommen. Sie hat hierfür die technischen Grundlagen von Google Glass knapp, verständlich und für die folgende Bewertung ausreichend dargestellt. In vier selbst erarbeiteten Szenarien werden sodann die künftigen Nutzungsmöglichkeiten repräsentativ beschrieben und daraus das Nutzen- und Gefahrenpotenzial überzeugend herausgearbeitet. Auf dieser Grundlage bietet die Arbeit eine systematische, vollständige und überzeugende datenschutzrechtliche Bewertung von Google Glass. Aus ihrer juristischen Bewertung entwickelt Frau Hohmann kreativ und originell technische Gestaltungsvorschläge zur Verbesserung der Datenschutzkonformität von Google Glass.

Die hier vorgelegte Masterarbeit der Universität Kassel im Studiengang Wirtschaftsrecht hat damit am Beispiel von Google Glass eine wesentliche Grundlage dafür gelegt, die Chancen und die Risiken von Wearable Computing zu erkennen und aus dem Blickwinkel der Grundrechte und des Datenschutzes zu bewerten. Sie hat außerdem

gezeigt, dass und wie eine Datenbrille grundrechts- und datenschutzverträglich gestaltet werden kann, sodass die Risiken weitgehend vermieden und die erhaltenswerten Funktionen genutzt werden können. Auf den in der Arbeit geleisteten theoretischen Vorarbeiten und orientiert an diesem gelungenen Beispiel rechtswissenschaftlicher Technikgestaltung können künftige Projekte zur Gestaltung von Wearable Computing aufsetzen. Da Frau Hohmann das sehr anspruchsvolle und überdurchschnittlich schwierige Thema in hervorragender Weise bearbeitet hat, wurde ihre Untersuchung mit der Bestnote und dem Preis für die beste Masterarbeit im Studiengang Wirtschaftsrecht des Jahres 2015 ausgezeichnet.

Dezember 2015

Für die Herausgeber *Prof. Dr. Alexander Roßnagel*

Übersicht

Abkürzungsverzeichnis

a. A.	anderer Ansicht
ABl.	Amtsblatt
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
Alt.	Alternative
App	Applikation
Art.	Artikel
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BeckRS	Beck-Rechtsprechung
Beil.	Beilage
BetrVG	Betriebsverfassungsgesetz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BPersVG	Bundespersonalvertretungsgesetz
bspw.	beispielsweise
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
bzgl.	bezüglich
bzw.	beziehungsweise
c‘t	Magazin für Computertechnik

ca.	circa
cm	Zentimeter
CR	Computer & Recht
d. h.	das heißt
DANA	Datenschutznachrichten
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DS-GVO	Datenschutzgrundverordnung
DSRL	Datenschutzrichtlinie (95/46/EG)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
e. V.	eingetragener Verein
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
Einf.	Einführung
Einl.	Einleitung
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention)
endg.	endgültig
ErfK	Erfurter Kommentar
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechte-Zeitschrift
EUV	Vertrag über die Europäische Union
evtl.	eventuell

EWR	Europäischer Wirtschaftsraum
f., ff.	folgende/-r/-s
FAZ	Frankfurter Allgemeine (Zeitung)
gem.	gemäß
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
Glass-Träger	Google Glass-Träger
GPS	global positioning system
GRC	Charta der Grundrechte der Europäischen Union (Grundrechtecharta)
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
Hdb DS	Handbuch Datenschutzrecht
HFR	Höchstrichterliche Finanzrechtsprechung (Zeitschrift)
Hrsg.	Herausgeber/in
HS	Halbsatz
i. d. R.	in der Regel
I&K-Dienste	Informations- und Kommunikationsdienste
I&K-Techniken	Informations- und Kommunikationstechniken
i. R. v.	im Rahmen von
i. S. v.	im Sinne von
i. S. d.	im Sinne des
i. V. m.	in Verbindung mit

Inc.	Incorporation
IP	Internet-Protokoll
IT	Informationstechnik
K&R	Kommunikation & Recht (Zeitschrift)
Kap.	Kapitel
KOM	Dokument der EU-Kommission
KUG	Kunsturhebergesetz
LG	Landgericht
lit.	Buchstabe
m. w. N.	mit weiteren Nachweisen
MMR	Multi-Media-Recht (Zeitschrift)
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
NSA	National Security Agency USA
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
NZV	Neue Zeitschrift für Verkehrsrecht
o. A.	ohne Autor
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
RDV	Recht der Datenverarbeitung (Zeitschrift)
Rn.	Randnummer
S.	Satz oder Seite

Slg.	Sammlung der Rechtsprechung des Gerichtshofes und des Gerichts Erster Instanz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u.a.	unter anderem
US	United States
USA	United States of America
USB	Universal Serial Bus
v.	von/vom
VG	Verwaltungsgericht
vgl.	vergleiche
VuR	Verbraucher und Recht – Zeitschrift für Wirtschafts- und Verbraucherrecht
WLAN	Wireless Local Area Network
WP	Working Paper (der Artikel 29-Datenschutzgruppe)
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZUM	Zeitschrift für Urheber- und Medienrecht

1 Einleitung

Die anhaltenden Technologietrends sorgen für eine fortschreitende Informatisierung der Welt. Zugleich stellen diese, durch die immer wieder neuen Entwicklungen der Informations- und Kommunikationstechniken (I&K-Techniken), große Herausforderungen für das Recht, im Besonderen für das Datenschutzrecht, dar. Dies gilt speziell für den Bereich des Ubiquitous Computing. Ungeachtet der informationellen Selbstbestimmung des Einzelnen,[1] dringen die I&K-Techniken in alle Lebensbereiche des Menschen ein und bieten für fast alle Situationen unbemerkt und ungefragt Unterstützung oder Informationen.[2] Diese allgegenwärtige Datenverarbeitung findet sich bereits in vielen Alltagsgegenständen wieder, die mit Sensor-, Kommunikations- und Rechnertechnik ausgestattet sind. Die Informationstechnik rückt dabei immer näher an den Menschen heran. Überwiegend sind elektronische Geräte in miniaturisierter Form in Kleidung, Smartwatches, Datenbrillen und Fitnessarmbändern enthalten, sodass bereits von Wearable Computing gesprochen werden kann. Durch diese Gadgets wird den Menschen ein intuitiver, müheloser und unmittelbarer Zugang zu beliebigen Informationen bereitgestellt sowie Online-Kontakt zu Informationsdiensten und anderen Menschen oder Alltagsgegenständen ermöglicht. Gleichwohl sollen die am Körper getragenen Computer viele Vorteile gegenüber Devices wie Smartphones und Tablets bringen sowie eine noch intensivere Verflechtung unserer physikalischen und digitalen Welt erlauben.

Die Nachfrage nach den Wearable Computern wächst aktuell rasant, und auch die Aussichten für die Zukunft sind erfolgsversprechend. Dabei zielt die Gerätegeneration, die jetzt mit Macht auf die Weltmärkte drängt, stark auf Lifestyle und Alltagsgebrauch ab.[3] Um dem Informationszeitalter gerecht zu werden, entwickelte der Internetkon-

---

1 In der gesamten Arbeit wird ausschließlich der maskuline Terminus gewählt.
2 *Roßnagel/Jandt/Skistims/Zirfas*, Datenschutz bei Wearable Computing, S. 1
3 *Dziemba/Wenzel*, # wir, Wie die Digitalisierung unseren Alltag verändert, S. 87.

zern Google Inc. seine Datenbrille Google Glass. Diese vereint einen mit dem Internet verbundenen Computer und eine Kamera in einem Brillengestell, das per Sprachbefehl bedient werden kann. Diese neue Technologie ist bereits in den USA sowie Großbritannien auf dem Markt und soll im Jahr 2015 in Deutschland erhältlich sein.[4]

1.1 Problemstellung der Arbeit

Während Google Glass als trendiges, cooles und modisches Accessoire angeboten wird, darf das dadurch resultierende rechtliche Gefahrenpotenzial nicht außer Acht gelassen werden.[5] Dies gilt insbesondere für das Persönlichkeitsrecht und den Datenschutz. Durch die vielseitigen Funktionen und der Kamera direkt vor dem Auge, wächst die Furcht durch das Blickfeld von Google Glass völlig gläsern zu sein. Die Zwecke, die mit Google Glass erreicht werden können, widersprechen den Zielen, die mit den Prinzipien des europäischen und deutschen Datenschutzrechts verfolgt werden.[6] Angesichts des rechtlichen Gefahrenpotenzials ist zu hinterfragen, ob trotz dieser dynamischen Technikentwicklung die Privatsphäre und das Recht auf informationelle Selbstbestimmung gewährleistet werden kann. Im Hinblick auf den bevorstehenden Verkaufsstart in Deutschland befasst sich diese Arbeit mit der Fragestellung, inwiefern das normative Schutzkonzept des Bundesdatenschutzgesetzes greift und wie die Zulässigkeit von Google Glass im Alltag aus datenschutzrechtlicher Sicht zu bewerten ist.

1.2 Gang der Untersuchung

Im nachfolgenden Kapitel werden in Anbetracht der oben geschilderten Problematik die Begrifflichkeiten des Ubiquitous sowie Wearable Computing näher beschrieben und die technischen Grundlagen von

---

4 Vgl. *dpa*, o. A., FAZ.NET v. 15.01.2015; *Wilkens*, heise-online v. 16.01.2015, Internetquelle.

5 *Solmecke/Kocatepe*, ZD 2014, 22

6 *Roßnagel/Jandt/Skistims/Zirfas*, Datenschutz bei Wearable Computing, S. 4.

Google Glass dargestellt. Im Anschluss werden in Kapitel 3 mögliche Szenarien mit Google Glass im Alltag vorgestellt, die im Laufe der Arbeit unter datenschutzrechtlichen Gesichtspunkten bewertet werden. In Kapitel 4 werden die rechtlichen Gefahrenpotenziale, die bei einer alltäglichen Nutzung von Google Glass für das Persönlichkeitsrecht und den Datenschutz entstehen, aufgeführt. Kapitel 5 stellt die Grundlagen des Datenschutzrechts auf internationaler, europäischer und nationaler Ebene vor und zeigt auf, wie die Eingriffe in das verfassungsrechtlich geschützte Persönlichkeitsrecht im Einzelnen ausgestaltet sind. Daran anknüpfend findet in Kapitel 6 anhand der Vorschriften des BDSG die datenschutzrechtliche Bewertung der in Kapitel 3 erläuterten Szenarien statt. Unter Berücksichtigung des rechtlichen Gefahrenpotenzials und der Ergebnisse der datenschutzrechtlichen Zulässigkeitsprüfung, werden in Kapitel 7 mögliche Gestaltungsvorschläge im Rahmen des Privacy by Design aufgeführt. Zusammengefasst werden die Ergebnisse im Fazit mit Blick auf den zukünftigen Einsatz von Google Glass.

2 Ubiquitous Computing

Der Begriff des „Ubiquitous Computing“ lässt sich auf Mark Weiser zurückführen, der bereits 1990 seine Vision einer Welt allgegenwärtiger Rechnertechnik vorstellte. Nach seinen Vorstellungen verschwindet der (Personal-) Computer als spezifisches Gerät und wird durch „intelligente Gegenstände“ ersetzt, welche die Menschen im Rahmen ihres alltäglichen Lebens und Tätigkeiten unbemerkt begleiten und unterstützen.[7] Ubiquitous Computing, bedeutet die Allgegenwärtigkeit von kleinsten, miteinander drahtlos vernetzten Computern, die unsichtbar in beliebige Alltagsgegenstände eingebaut werden oder an diese angeheftet werden können.[8] Vor allem die fortschreitende Miniaturisierung aller technischen Komponenten wie Prozessoren, Sensoren, Aktoren, Mikrofone, Kameras, Rechenleistung, die Fortschritte bei der autarken Energieversorgung sowie die günstige Verfügbarkeit von Computerhardware ermöglichen diese Allgegenwärtigkeit.[9] Infolgedessen verschwindet der Computer als spezifisches Gerät weitgehend aus der alltäglichen Welt, während zunehmend Alltagsgegenstände mit umfassender Rechenleistung in den Vordergrund gelangen.[10]

Durch die Integration in Alltagsgegenstände ist diese Technologie nicht mehr erkennbar, sondern stellt eine unterstützende proaktive Hintergrundassistenz, die weitgehend autonom agiert, zur Verfügung.[11] Im Vordergrund steht dabei die Vernetzung von Komponenten und Diensten, die Interaktion der Komponenten und Benutzer un-

---

7 *Weiser*, Scientific American, 265, 94.

8 *Solmecke/Vondrlik*, MMR 2013, 755, *Ferscha*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 3 (10); *Roßnagel*, in: Bizer/v. Mutius/Petri/Weichert (Hrsg.), Innovativer Datenschutz, S. 335 (341).

9 Siehe dazu ausführlich *Timmermann/Beigl/Handy*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 61 ff.; *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 11; *Boeing/Stieler*, Technology Review, 10/2014, S. 26 (27); *Wright/Steventon*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 17.

10 *Mattern*, in: Mattern (Hrsg.), Total vernetzt, S. 1 (3 ff.); *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 9; *Maurer*, Informatik-Spektrum, 2004, 44.

11 *Ferscha*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 3 (5).

tereinander sowie die Kontrolle bzw. Koordination dieser Interaktion. Dazu gehört u. a. auch die Identität und Authentifizierung der Komponenten, das Anbieten und Auffinden von Diensten, die Koordination lokaler Aktivitäten, Umgebungskenntnis, Kontextbezogenheit etc.[12] Ziel des Ubiquitous Computing ist es, dem Menschen in jeder Situation seines Alltags um die Möglichkeiten der digitalen Informationswelt, die ihn unsichtbar umgeben, in seinen Handlungsmöglichkeiten unbemerkt zu bereichern.[13] Daraus folgt eine allgegenwärtige Informationsverarbeitung und damit einhergehend die Möglichkeit, jederzeit von beliebiger Stelle aus auf Daten zu zugreifen,[14] sodass auch die Erhebung und Verarbeitung personenbezogener Daten fast unbeschränkt erfolgen kann.[15] Die Kombination der Miniaturcomputer mit Sensoren dient dazu, die Umwelt der Gegenstände umfänglich zu erfassen und diese mit Informationsverarbeitungs- und Kommunikationsfähigkeiten auszustatten. Passive und praktisch unsichtbare Elektronik machen es zudem möglich Dinge bzw. Gegenstände in der Ferne präzise zu lokalisieren, mit diesen zu kommunizieren sowie zu erkennen, wo sie sich z. B. befinden, welche anderen Gegenstände in der Nähe sind und was mit ihnen gerade geschieht bzw. in der Vergangenheit geschah.[16] Diese selbstorganisierende Verbindung der Gegenstände, die Zusammenführung und Sammlung der Informationen führt schließlich zu einer umfänglichen Verknüpfung vieler verschie-

---

12 *Ferscha*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 3 (5); *Roßnagel*, in: Bizer/v. Mutius/ Petri/Weichert (Hrsg.), Innovativer Datenschutz 1992-2004, S. 335 (342).

13 *Ferscha*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 3 (8); *Roßnagel/Müller*, CR 2004, 625 (628); *Roßnagel*, in: Bizer/v. Mutius/Petri/Weichert, Innovativer Datenschutz, S. 335 (341).

14 *Mattern*, Informatik-Spektrum 2001, 145.

15 *Roßnagel*, in: Bizer/v. Mutius/Petri/Weichert (Hrsg.), Innovativer Datenschutz, S. 335 (336).

16 *Mattern*, in: Roßnagel/Sommerlatte/Winand (Hrsg.), Digitale Visionen, S. 11; *Mattern*, in: Mattern (Hrsg.), Total vernetzt, S. 1 (20); *Baumeler*, Von kleidsamen Computern und unternehmerischen Universitäten, S. 1; *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 11; *Pfaff/Skiera*, in: Britzelmaier/Geberl/Weinmann (Hrsg.), Der Mensch im Netz, S. 26; so auch schon *Roßnagel*, in: Bizer/v. Mutius/ Petri/Weichert (Hrsg.), Innovativer Datenschutz 1992-2004, S. 335 (336).

dener Bereiche des menschlichen Lebens.[17] Dadurch wird die Art des Zugangs zu Informationen stark beeinflusst, da die Informationsverarbeitung dem Nutzer schnell einen effizienten und sicheren Zugang gewährt, unabhängig von Zeit und aktuellem Standort.[18] Ubiquitous Computing findet man zunehmend in der näheren Umgebung des Menschen, so werden z. B. Thermostate und Stromzähler, Autos und Straßen und weitere Alltagsgegenstände wie Möbel und Kühlschränke nachgerüstet, damit sie sich unablässig im Netz mitteilen können.[19] Viele Produkte sind bereits heute nicht mehr nur eine Alltagsunterstützung, sondern werden sogar zum persönlichen Lebensberater, zum Fitness-Trainer oder zur Haushaltshilfe.[20]

Allerdings darf bei Ubiquitous Computing der Aspekt „Schutz der Privatsphäre" nicht unbeachtet bleiben. Ubiquitous Computing bietet nicht nur vielfältige Unterstützungen und Erleichterungen für den Menschen, sondern gefährdet gleichzeitig seine informationelle Selbstbestimmung.[21] Smarte Gegenstände und die sensorbestückte Umgebung sind fast immer aktiv und sammeln eine Unmenge von Daten, um den Nutzern sinnvolle Dienste anbieten zu können. Insoweit offenbart sich in einer ubiquitären Welt ein detailliertes Bild über die Interessen, die Neigungen, die allgemeine Verfassung und auch über die Schwächen einer Person.[22] Aus diesem Grund wirft das Leben in „smarten Umgebungen" unbedingt auch die eminent wichtige Frage nach dem Datenschutz auf.

---

17 *Roßnagel/Müller*, CR 2004, 625 (626).

18 Siehe *Hansmann, U./Merk, L./Nicklous, M.S./Stober, T.*, Pervasive Computing Handbook.

19 *Boeing/Stieler*, Technology Review, 10/2014, S. 26 (27); *Roßnagel/Jandt/Skistims/Zirfas*, Datenschutz bei Wearable Computing, S. 1; *Solmecke/Vondrlik*, MMR 2013, 755; *Schmidt*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 77 (82).

20 *Solmecke/Vondrlik*, MMR 2013, 755.

21 *Roßnagel*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 265 (272).

22 *Mattern*, in: Mattern (Hrsg.), Total vernetzt, S. 1 (31); *Linnhoff-Popien*, in: Eberspächer/v. Reden, Umhegt oder abhängig?, S. 35 (47); *Roßnagel/Müller*, CR 2004, 625 (627).

2.1 Wearable Computing

Ein wichtiges Anwendungsfeld des Ubiquitous Computing ist das Wearable Computing. Der Begriff des Wearable Computing kann als tragbarer, anziehbarer oder sogar kleidsamer Rechner verstanden werden.[23] Kein Alltagsgegenstand ist dem Menschen so nahe wie seine Kleidung, die immer bei ihm ist, all seinen Bewegungen folgt und hautnah dasselbe erlebt.[24] Daher liegt es nahe, neben Alltagsgegenständen auch die Funktionalität der Kleidung zu erweitern und so zu sensibilisieren, dass sie unser Verhalten und z. B. unsere Gesundheit beobachtet, den Menschen als persönlicher Assistent tagtäglich begleitet und auf vielseitigste Weise unterstützt.[25] Die technischen Entwicklungen im Rahmen des Ubiquitous Computing machen es möglich Bekleidungsgegenstände, Accessoires sowie Brillen mit elektronischen Geräten in miniaturisierter Form auszustatten und so etwa Kameras, Sensoren und andere elektronische Komponenten permanent am menschlichen Körper zu tragen.[26] Als ständige Begleiter erweitern oder ermächtigen die Wearable Computer den Benutzer, indem sie den Kontext des Benutzers erfassen, auswerten und ihm als universelles Werkzeug den gesamten Tag nützlich sind ohne ihn zu behindern oder zu stören.[27] Sie sind gekennzeichnet durch die Fähigkeit „von sich aus" Verhalten und Aktivitäten des Benutzers sowie äußere Situationen zu erkennen und diese Information zu nutzen, um Konfiguration und Funktionalität des Systems dem jeweiligen Benutzerbedürfnis und der Benutzersituation anzupassen.[28] Dadurch ist es möglich, dem Nutzer mehr Sicherheit zu geben, seine Sinne zu erweitern, sein Ge-

---

23 *Ziegler*, c't 21/2002, 102; *Baumeler*, Von kleidsamen Computern und unternehmerischen Universitäten, S. 3; *Klug*, Prozessunterstützung für den Entwurf von Wearable-Computing-Systemen, S. 9.

24 *Tröster*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 103.

25 *Tröster*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 103.

26 *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 11; *Mattern*, in: Roßnagel/Sommerlatte/Winand (Hrsg.), Digitale Visionen, S. 3 (13); *Maurer*, Informatik-Spektrum, 2004, 44 (45).

27 *Klug*, Prozessunterstützung für den Entwurf von Wearable-Computing-Systemen, vii, S. 10, 13.

28 *Tröster*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 103 (115 f.).

dächtnis zu unterstützen und ihm seine Arbeit bzw. seinen Alltag zu erleichtern.[29]

Grundsätzlich können dadurch neuartige Interaktionsformen zwischen Mensch und Technik genutzt werden. Z. B. können Kleider aus Stoffen, die leitfähige Fasern enthalten, beim Dehnen ihren Widerstand ändern und dadurch Körperbewegungen erfassen oder Funktionen durch ein leichtes Ziehen an einem Stück der Kleidung auslösen.[30] Des Weiteren sind sie u. a. fähig, Körper- und Umgebungsdaten zur medizinischen Kontrolle zu erfassen und zu verarbeiten.[31] Zu den aktuellen Wearable Computing Gadgets zählen Smartwatches wie die Armbanduhr Galaxy Gear von Samsung,[32] das Datenarmband Jawbone UP24,[33] Fitness-Armbänder[34] oder Datenbrillen wie der Untersuchungsgegenstand Google Glass.[35] Smartwatches reagieren auf Berührung und Stimme, sodass Termine notiert, neue Nachrichten abgerufen bzw. auch Anrufe getätigt werden können. Fitness-Armbänder helfen, gekoppelt mit Smartphone-Apps, die Körperaktivität zu analysieren und dementsprechende Tipps zum Wohlbefinden zu geben.[36] Die einzelnen Funktionen der Datenbrille Google Glass werden im Folgenden ausführlicher erläutert.

2.2 Einführung in die technischen Grundlagen von Google Glass

Während zuvorderst eine allgemeine Darstellung des Wearable Computing stattfand, wird in diesem Abschnitt ein kurzer Einblick in die

---

29 Vgl. zu diesen Träumen, die für die Nutzung von Ubiquitous Computing bedeutsam sein werden *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 13 ff.; *Maurer*, Informatik-Spektrum 2004, 44 (50).

30 *Mattern*, in: Mattern (Hrsg.), Total vernetzt, S. 1 (13); *Tröster*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 103 (112).

31 Z. B. bei Schutzanzügen siehe *Roßnagel/Jandt/Skistims/Zirfas*, Datenschutz bei Wearable Computing, S. 1; *Tröste*r, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 103.

32 Samsung Galaxy Gear, Internetquelle.

33 Jawbone Up24, Internetquelle.

34 Siehe zum Überblick, *Kremp*, Spiegel Online v. 26.04.2014.

35 Google Glass, Internetquelle.

36 *Kremp*, Spiegel Online v. 26.04.2014.

technischen Grundlagen und Funktionen des Untersuchungsgegenstandes Google Glass gegeben. Anhand dieser Informationen wird in den folgenden Kapiteln die juristische Analyse durchgeführt.

Bei Google Glass handelt es sich um eine Art Brille, an deren Gestell ein Miniaturcomputer montiert ist. Die Verbindung via Bluetooth mit einem Smartphone ermöglicht die Internetverbindung, sodass mittels eines Glasprismas verschiedene Informationen im oberen Sichtfeld des Trägers vor dem rechten Auge eingeblendet werden können.[37] Durch den direkt am Auge angebrachten Minibildschirm, bekommt der Google Glass-Träger (Glass-Träger) das Gefühl vermittelt, im rechten oberen Blickfeld einen ca. 20 cm großen Bildschirm zu sehen.[38]

Grundsätzlich könnte die Datenbrille zumindest im WLAN autark arbeiten, jedoch wird ein Smartphone mit der sogenannten Companion-App „MyGlass" benötigt, um umfassend alle Funktionen nutzen zu können.[39] Die MyGlass-Seite[40] und die MyGlass-App dienen der Verwaltung von Google Glass-Anwendungen, auch Glassware genannt.[41] Zu diesen Anwendungen gehören u. a. Google Plus, Gmail, Facebook etc.[42] All diese Apps von Drittanbietern nutzen Googles Mirror-API, womit sich Web-Anwendungen für die Datenbrille programmieren lassen, die ihre Inhalte von Google-Servern auf das Brillen-Display schicken.[43] Durch die Anbindung an die Google Infrastruktur sowie Dienste Dritter, die ähnlich wie bei Smartphones mit Apps auf dem Gerät ausgeführt werden, entfaltet Google Glass erst das volle Potenzial.[44] Google Glass ermöglicht dem Träger, die zahlreichen, komple-

---

37 *Llorente/Morant*, in: Peris-Ortiz/Garrigòs-Simòn/Pechuán (Hrsg.), Innovation and Teaching Technologies, S. 127 (130); *Solmecke/Kocatepe*, ZD 2014, 22; *Weichert*, DANA 2/2013, 53; *Bendel*, Informatik-Spektrum Herbst 2014, 1 (4).

38 *Weichert*, DANA 2/2013, 53.

39 *Porteck/Sokolov/Zota*, c't 13/2013, 62 (64, 66); siehe dazu MyGlass Support, Internetquelle.

40 MyGlass Support, Internetquelle.

41 Glassware, Internetquelle.

42 Siehe dazu Google Glass Application List, Internetquelle.

43 *Porteck/Sokolov/Zota*, c't 13/2013, 62 (66).

44 Start building great Glassware, Internetquelle.

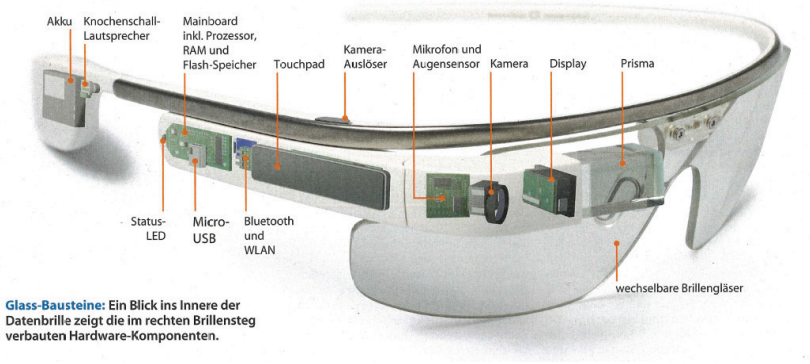
xen Funktionen eines Smartphones zu nutzen, ohne dieses dafür in die Hand nehmen zu müssen.[45] Insoweit stellt die Datenbrille eine Art Erweiterung für Smartphones dar, sofern man die Brille per Bluetooth daran koppelt. Dabei können, neben der Funktion als Headset, auf dem Prisma über dem rechten Auge Termine, Nachrichten, die Wetterlage oder der Weg zum nächsten Café eingeblendet werden.[46] Weiter ist es durch den umfassenden Zugang zum Internet möglich Texte, Dokumente, Bilder und akustische Samples hoch- und runterzuladen.[47]

Wer eine Korrekturbrille benötigt, kann für 225 US-Dollar vier unterschiedliche Korrektur-Brillengestelle erwerben, auf die man die Elektronik der Google Glass schrauben kann. Die Brillen sind ab Werk mit ungeschliffenen Gläsern ausgestattet, die dann vom Optiker durch individuelle Korrekturgläser ersetzt werden. Laut Google sind Glasstärken von bis +- 4 Dioptrien realisierbar.[48]

Wie die nachfolgende Abbildung zeigt, ist es mit der integrierten 5-Megapixel-Kamera möglich, Fotos zu machen und Videos mit 720p[49] zu erstellen.[50] Beim Fotografieren oder Filmen leuchtet das Prisma auf, damit der Einsatz für das Gegenüber nicht unbemerkt bleibt.[51] Über ein Mikrophon sind Spracheingaben und Tonaufnahmen möglich.[52] Hinter dem Ohr befindet sich ein Knochenschall-Lautsprecher über den, ähnlich wie bei Hörgeräten, die Tonausgaben direkt auf den Schädelknochen übertragen werden.[53] Dadurch wird es u. a. möglich zu telefonieren und Videokonferenzen abzuhalten.[54] Der Flash-

45 *Weichert*, DANA 2/2013, 53 (54); *Schwenke*, K&R 2013, 685.
46 *Porteck/Sokolov/Zota*, c't 13/2013, 62 (63).
47 *Weichert*, DANA 2/2013, 53.
48 *Janssen*, c't 6/2014, 74.
49 720p-Signale werden mit einer Auflösung von 1280×720 Pixeln übertragen und ergeben ein Videosignal von 720 Linien.
50 *Weichert*, DANA 2/2013, 53; *Porteck/Sokolov/Zota*, c't 13/2013, 62 (65).
51 *Porteck/Sokolov/Zota*, c't 13/2013, 62, (65).
52 *Weichert*, DANA 2/2013, 53.
53 *Porteck/Sokolov/Zota*, c't 13/2013, 62 (64); *Weichert*, DANA 2/2013, 53.
54 *Weichert*, DANA 2/2013, 53.

Speicher ist 16 Gigabyte groß, wovon 12 Gigabyte dem Nutzer zur Verfügung stehen.[55] Der Akku soll ohne Nachladen einen ganzen Tag betriebsfähig sein. Geladen wird über ein mitgeliefertes Ladegerät mit Mikro-USB-Anschluss.[56] Am Ende des Bügels sitzt der Akku.[57]



Glass-Bausteine: Ein Blick ins Innere der Datenbrille zeigt die im rechten Brillensteg verbauten Hardware-Komponenten.

Quelle: *Porteck, S./Sokolov, D./Zota, V.*, c't 13/2013, S. 64.

Die Menüführung erfolgt durch Kopfbewegungen, Wischen und Tippen auf den rechten Brillenbügel, der nicht nur Technik aufnimmt, sondern auch ein Touchpad enthält.[58] Mit Vor- bzw. Zurückstreichen wandert man durch kleine Kacheln und wählt eine Funktion durch Antippen aus. In Listen kann man auch durch Heben und Senken des Kopfes scrollen.[59] Die (derzeit nur englischen) Sprachbefehle werden mit dem Stichwort „OK, Glass" eingeleitet. Anschließend folgen die eigentlichen Befehle „google" (für die Suche), „take a picture" (Fotografieren), „record a video" (Videoaufnahme), „get direction (to)" (Navigation wahlweise für Auto-, Fahrradfahrer oder Fußgänger), „send a message (to)" (Versand von SMS, E-Mail), „make a call (to)"

---

55 *Porteck/Sokolov/Zota*, c't 13/2013, 62 (63); *Weichert*, DANA 3/2013, 53.
56 *Janssen*, c't 15/2013, 76 f.; *Weichert*, DANA 2/2013, 53.
57 *Porteck/Sokolov/Zota*, c't 13/2013, 62 (64).
58 *Janssen*, c't 2014/6, 74; *Weichert*, DANA 2/2013, 53; *Porteck/Sokolov/Zota*, c't 13/2013, 62 (64); *Kremp*, Spiegel Online v. 07.06.2013.
59 *Porteck/Sokolov/Zota*, c't 13/2013, 62 (65).

(Telefonanruf) oder „hangout with" (Google+ Hangout).[60] Zudem soll Google Glass fähig sein, über Augenbewegungen (z. B. Zwinkern) gesteuert zu werden.[61]

Sämtliche Informationen bzw. Daten wie Inhalte, Verkehrsdaten und Personenzuordnungen werden per Internetverbindung auf Google-Server übertragen. Mit Hilfe der Google-Server werden diese Informationen von dem US-Unternehmen verarbeitet, zurück an die Brille geschickt und in das Sichtfeld der Brille projiziert.[62] So können Glass-Träger z. B. ihre Videoaufnahmen mit Googles Cloud-Speicher synchronisieren, sie direkt mit Dritten teilen oder im Internet und sozialen Netzwerken veröffentlichen.[63]

Die Beta-Version von Google Glass hat sich bereits diversen Langzeittests unterziehen müssen, mit dem Endergebnis, das die Technologie noch nicht vollends ausgereift ist und nicht zuverlässig und richtig funktioniert.[64] Viele Funktionen die Google Glass bisher bietet, können ebenso von Smartwatches oder einem Smartphone samt Headset erledigt werden. Jedoch scheint Google Glass die Brille der Zukunft zu sein, indem sie Mobiltelefon, Fotoapparat und Videokamera kombiniert und ständig mit dem Internet verbunden ist.[65]

---

60 *Solmecke/Kocatepe*, ZD 2014, 22; *Porteck/Sokolov/Zota*, c't 2013/13, 62 (63).

61 Siehe bereits *Maure*r, Informatik-Spektrum 27/2004, 44 (47); *Janssen*, c't 2014/6, 74; *Weichert*, DANA 2/2013, 53.

62 *Solmecke/Vondrlik*, MMR 2013, 755; *Solmecke/Kocatepe*, ZD 2014, 22 (23); *Ziegler*, c't 13/2013, 70.

63 Die Verbindung mit dem Smartphone ist notwendig, um alle Funktionen von Glass nutzen zu können, *Tung*, ZDnet v. 17.05.2013.

64 *Janssen*, c't 15/2013, 76.

65 Vgl. *Mattern*, in: Roßnagel/Sommerlatte/Winand (Hrsg.), Digitale Visionen, S. 1 (13).

3 Mögliche Szenarien mit Google Glass im Alltag

Die Datenbrille von Google soll für jedermann von Nutzen sein und sich geschmeidig in den Alltag einfügen.[66] Wie ein Alltag mit Google Glass aussehen könnte, zeigen die folgenden ausgewählten Szenarien. Dabei darf nicht außer Acht gelassen werden, dass die Kamera- und Tonaufnahme jederzeit unbemerkt erfolgen könnte. Unter Berücksichtigung des Beta-Stadiums von Google Glass und des Vorbehalts der Flexibilität möglicher Weiterentwicklung seitens Google sind die Szenarien an mancher Stelle hinsichtlich Funktionalität und Anwendungen frei konstruiert. Dennoch lässt sich aufgrund der schnellen und stetigen Entwicklung der technischen Möglichkeiten die Realisierung dieser Szenarien nicht völlig ausschließen.

3.1 Google Glass beim Sport

Den aktuellen Schönheits- und Fitness-Trends ist es zu verdanken, dass es eine Vielzahl an verschiedenen Apps für Smartphones gibt, die bei dem individuellen Fitnesstraining unterstützend zur Seite stehen.[67] Wird das Smartphone an Google Glass gekoppelt, könnte das Training noch viel erfolgreicher gestaltet werden. Der lästige Blick auf das Smartphone-Display könnte vermieden werden, wenn die Datenbrille die notwendigen Informationen direkt im Blickfeld anzeigen würde. Ein freihändiges Training wäre problemlos möglich, indem Google Glass die Trainingsanweisungen sowie Korrekturhinweise für eine bestimmte Sportart oder Muskelgruppe direkt vor dem Auge einblendet. Ebenso könnten akustische Signale z. B. eines Takt- oder Schrittzählers mittels der Knochenschalllautsprecher besser aufgenommen werden, ohne auf Kopfhörer, die bei Bewegungen leicht aus dem Ohr fallen oder verrutschen, angewiesen zu sein. Ferner könnte Google Glass als ständiger Begleiter beim Joggen oder Radfahren zur Navigation ge-

[66] Allerdings muss man nach Google Glass Terms das 18. Lebensjahr erreicht haben, Internetquelle.

[67] Siehe z. B. tolle Fitness-Apps für Ihr Handy, Internetquelle.

nutzt werden, Geschwindigkeit und Höhenmeter einblenden sowie zusätzlich noch Fotos oder Videos von der Umgebung aus dem eigenen Blickfeld heraus aufnehmen.[68]

3.2 Google Glass als Flirthilfe

Trägt man Google Glass im Nachtleben, in der Diskothek oder Lokalen, könnten sich für Personengruppen wie Singles ganz neue Möglichkeiten eröffnen. Neben der Funktion, die beliebtesten Lokalitäten der Stadt, entsprechend der persönlichen Präferenzen für Musik sowie Publikum, schnell anzuzeigen, könnte Google Glass dem Nutzer auch gleichzeitig die jeweiligen Navigationshinweise dorthin liefern. In der Diskothek könnte Google Glass als eine Art „Flirthilfe" umfunktioniert werden. Mit Hilfe der Funktion der Gesichtserkennung[69] und der ständigen Verbindung zum Internet besteht die Möglichkeit eine interessante Person zu googeln oder diese sogar in einem sozialen Netzwerk wie Facebook zu identifizieren. Dadurch ist es möglich in kürzester Zeit wichtige Informationen über diese Person hinsichtlich Beziehungsstatus, Interessen, Alter etc. zu erhalten. Mit diesem Hintergrundwissen, könnte der Glass-Träger abschätzen, ob er diese Person kennen lernen möchte und ggf. anhand der Informationen ein entsprechendes Thema für eine Unterhaltung findet. Während eines Gesprächs ist es möglich Fotos oder sogar Videomitschnitte aufzunehmen und diese mit entsprechendem Zeit- und Ortstempel zu versehen, sodass sie im digitalen Tagebuch gespeichert werden können.[70]

3.3 Google Glass für beeinträchtigte Menschen

Wer bezüglich Beweglichkeit, Kommunikationsfähigkeit oder Gehör eingeschränkt ist, könnte eine enorme Erleichterung im Alltag durch Google Glass erfahren. Dies gilt insbesondere für die Benutzung ohne

---

68 Google Glass beim Sport, Internetquelle

69 Google schließt zwar die Funktion der Gesichtserkennung bisher aus, jedoch ist diese nicht gänzlich ausgeschlossen, siehe google terms, Internetquelle.

70 So bereits *Maurer*, Informatik-Spektrum 27/2004, 44 (47).

Hände, und die Möglichkeit, die Interpretation von Gesichtsausdrücken zu erweitern.[71] Die Sprachsteuerung macht es möglich, dass auch Menschen mit einer starken körperlichen Behinderung durch Google Glass einen unkomplizierten Zugang zum Internet bekommen und einfacher an der Gesellschaft teilhaben können. Gleiches gilt für Menschen die an Autismus leiden, indem die Datenbrille bei der ohnehin eingeschränkten Kommunikationsfähigkeit behilflich ist, wenn diese bei der Interpretation und Erkennung von Emotionen, Gestik und Mimik unterstützend mitwirkt.[72] Zudem können Gehörlose und Schwerhörige von Live-Untertitel-Programmen auf der Google Glass profitieren. Google Glass könnte es ermöglichen, jedes Gespräch zu 100% in Echtzeit zu untertiteln.[73] Dadurch können Barrieren punktuell mit verschiedenen Programmen aus der Welt geschafft werden und eine kommunikative Basis für Hörbehinderte zwischen Hörenden eingerichtet werden.

3.4 Google Glass am Arbeitsplatz

Google Glass soll zunehmend am Arbeitsplatz eingesetzt werden, um dort spezifische Probleme zu lösen.[74] Dies gilt insbesondere für Mitarbeiter mit flexiblem Arbeitsplatz die beide Hände freihaben müssen und zugleich Zugang zu Informationen brauchen. In diesem Abschnitt sollen einige Arbeitsbereiche kurz vorgestellt werden, in denen Google Glass als nützliche Hilfe angedacht ist.

In der Logistikbranche können den Lagerarbeitern ihre Arbeitsaufträge in Echtzeit übermittelt und alle wichtigen Informationen dazu auf Google Glass angezeigt werden. Die Sprachsteuerung ermöglicht ein freihändiges und papierloses arbeiten, sodass Warenbewegungen unmittelbar im Lagerverwaltungssystem verzeichnet werden kön-

71 Siehe dazu Google Glass: eine Revolution für Behinderte, Internetquelle.
72 *Anthony*, ExtremeTech v. 04.09.2014.
73 *Straumann*, HearZone v. 14.07.2014, Internetquelle; siehe dazu die App *Caption*, Internetquelle.
74 *Miller*, The New York Times v. 08.04.2014, p. B1.

nen.[75] Google Glass liest die nötigen Informationen vor und blendet über das Display den Standort und die Warenmenge ein. Auch das Abscannen des Barcodes mit Hilfe der in der Datenbrille integrierten Kamera könnte möglich sein. Treten spezifische Probleme auf, können per Video-Chat Ansprechpartner oder Experten zugeschaltet werden, um z. B. eine Reparatur oder Wartung auch durch einen Laien mit Anweisungen eines Experten durchzuführen.[76]

Ein Einsatz im Krankenhaus lässt sich ebenfalls nicht ausschließen. Google Glass soll Ärzte unterstützen, indem sie eine Verbindung zu elektronischen Datenbanken herstellt. Dadurch ist es Ärzten möglich, während einer Operation Röntgenbilder, endoskopische Aufnahmen oder Herzfrequenzen ständig im Auge behalten zu können.[77]

Polizisten könnten mit Hilfe von Google Glass Verkehrssünder festhalten, indem der Polizist mit der Datenbrille das Autokennzeichen fotografiert und es mit einer Polizei-Datenbank abgleicht.[78] Weiter könnte man schnell und unkompliziert ein Video von einem Einsatz aufnehmen, um im Nachhinein die Situation genau darlegen zu können.[79] Mithilfe der Gesichtserkennungsfunktion wäre es möglich, gesuchte Straftäter zu identifizieren und gegen diese direkt vorzugehen.[80]

Feuerwehrmänner könnten mit Google Glass künftig schneller zu Einsatzorten finden sowie zusätzliche Informationen zu Gebäuden oder Fahrzeugen abrufen.[81]

---

75 Siehe Mindsquare GmbH v. 20.08.2014, Internetquelle.
76 *Bräutigam*, Der Deutsche Innovationspreis v. 02.06.2014, Internetquelle.
77 *Rojahn*, Technology Review v. 21.05.2014, Internetquelle; *Hardt*, FAZ.net v. 10.04.2014.
78 *Spata*, heise-online v. 22.05.2014, Internetquelle.
79 Vgl. mit den Schulterkameras der hessischen Polizei siehe dazu *dpa*, o. A., Focus Online v. 01.10.2014
80 *Paletta*, ZDF Online v. 08.02.2014.
81 *Költzsch*, golem v. 21.01.2014, Internetquelle

3.5 Kritische Würdigung

Die beschriebenen Szenarien verdeutlichen, warum Google Glass als technischer Meilenstein und Brille für das Informationszeitalter gesehen wird. Abgesehen von der technischen Innovation und den Vorteilen im Alltag für den Einzelnen, stößt die Datenbrille aus rechtlicher Sicht jedoch auf Kritik.[82] Diese Kritik ist darin begründet, dass jederzeit Kameraaufnahmen unbemerkt möglich sind und dadurch die Privatsphäre Dritter enorm verletzt wird. Es lässt sich nicht vermeiden, dass auf der Straße, in Lokalitäten, im Fitness-Studio oder auf dem Fußballplatz, von einer kontinuierlichen Aufnahme bzw. Überwachung ausgegangen werden muss. Zudem muss gerade bei Google Glass damit gerechnet werden, dass alles, das in das Aufnahmefeld der Datenbrille fällt in wenigen Sekunden im Internet zu sehen sein kann. Die jederzeit mögliche Ausrichtung eines Objektivs auf das Selbst, fördert eine permanente Anspannung. Dies trifft nicht nur bei der freizeitlichen bzw. sportlichen Tätigkeit zu, sondern auch in sensiblen Bereichen wie Umkleidekabinen, Duschen oder Toiletten.[83] Gerade in solch privaten Bereichen besteht eine erhöhte Gefahr von unerlaubtem Fotografieren, Filmen sowie intimstes Eindringen in die Privatsphäre Dritter. Insbesondere Glass-Träger, die evtl. nicht über das nötige Know-how und Verständnis dieser Technik verfügen, könnten durch Hackangriffe sogar selbst leicht zu Opfern von Missbrauch und Kriminalität durch ihre eigene Datenbrille werden.

Ebenso schwer wiegt, dass sich neben der möglichen Überwachung und des damit einhergehenden möglichen Datenmissbrauchs, auch das menschliche Miteinander ändert. Normalerweise dienen das Aufeinandertreffen von Personen und der Blickkontakt als Versicherung und Vertrauensbildung, doch durch das Tragen von Google Glass könnte dies eher als ein Angriff auf die Intimsphäre empfunden werden. Das zwischenmenschliche Verhältnis würde akut in Mitleiden-

[82] Vgl. *Weichert*, DANA 2/2013, 53
[83] *Ziegler*, c't 13/2013, 70; *Janssen*, c't 5/2013, 76 (77).

schaft gezogen und grundsätzlich in Frage gestellt.[84] Ferner sind die daraus resultierende Verhaltensveränderung oder sogar Manipulation zu nennen.[85] Davon sind zum einen die Menschen betroffen, die sich in der Gegenwart eines Glass-Trägers beobachtet fühlen und dementsprechend ihr Verhalten anpassen sowie der Nutzer selbst, der ggf. auch sein Verhalten aufgrund der von Google Glass gelieferten Hintergrundinformationen ändert. Dabei ist fraglich, inwiefern die Nutzer Google Glass unmerklich in das individuelle Verhalten und Handeln integrieren und dabei immer mehr das Menschsein gegen die Rolle eines „Cyborgs"[86] ersetzen.[87]

84 *Bendel*, Informatik-Spektrum Herbst 2014, 1 (4).
85 *Roßnagel,* Datenschutz in einem informatisierten Alltag, S. 86 f.
86 Ein Mischwesen aus Mensch und Maschine, Internetquelle.
87 *Roßnagel,* Datenschutz in einem informatisierten Alltag, S. 86.

4 Rechtliches Gefahrenpotenzial

Die eben geschilderten Szenarien legen dar, dass die Funktionen und Einsatzgebiete von Google Glass aus rechtlicher Sicht mit vielen Gefahren verbunden sind. Dies gilt insbesondere für das Privat- und Familienleben, das allgemeine Persönlichkeitsrecht mit seinen einzelnen Ausprägungen sowie für den Datenschutz. Begründen lassen sich diese Gefahren durch die mangelnde Transparenz beim Erfassungsvorgang, der Qualität und Quantität der erfassten Daten sowie der mögliche Kontrollverlust und die Unvorhersehbarkeit der weiteren Nutzung der Daten.[88] Wie sich das rechtliche Gefahrenpotenzial im Einzelnen rechtfertigen lässt, zeigen die folgenden Ausführungen.

4.1 Mangelnde Transparenz beim Erfassungsvorgang

Durch Google Glass können in unmerklich und vielfach undurchschaubarer Weise nahezu überall und fast immer personenbezogene Daten in einem sehr großen Umfang erhoben und weitergegeben werden, damit sie für vielfältigste Zwecke genutzt werden können.[89] Diese intransparente Datenerhebung lässt sich darauf zurückführen, dass es anders als bei der bisherigen Kameraaufnahme mit Smartphone oder Kamera kein Anvisieren mehr benötigt. Google Glass befindet sich bereits vor den Augen, sodass es an einer eindeutigen Aufnahmegeste fehlt.[90] Völlig unbemerkt bleibt eine Aufnahme aus der Nähe zwar nicht, da man dafür den entsprechenden Sprachbefehl äußern muss sowie das Prisma beim Fotografieren und Filmen aufleuchtet.[91] Allerdings können Aufnahmen ebenfalls in wenigen Sekunden und mit den entsprechenden Apps automatisch ausgelöst werden, z. B. wenn eine Person den Raum betritt oder sogar per Augenzwinkern.[92]

---

88 *Schwenke*, in: Taeger (Hrsg.), Law as a Service, Tagungsband DSRI-Herbstakademie, S. 215 (217).

89 *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 85.

90 *Schwenke*, K&R 2013, 685 (686); *Solmecke/Kocatepe*, ZD 2014, 22.

91 *Solmecke/Kocatepe*, ZD 2014, 22; *Porteck/Sokolov/Zota*, c't 13/2013, 62 (65); *Schwenke*, K&R 2013, 685 (686); *Weichert*, DANA 2/2013, 53 (54); *Ziegler*, c't 13/2013, 70 (71).

92 *Schwenke*, K&R 2013, 685 (686).

Durch die Leichtigkeit der Aufnahmefunktion geraten Persönlichkeitsrechte Dritter aus dem Blickfeld der Glass-Träger, da ihnen de facto keine Möglichkeit geboten wird, um über die Zulässigkeit des Aufnahmevorgangs nachzudenken.[93] Für die Betroffenen ist es unmöglich im Voraus zu wissen, wer welche Daten erhebt, nutzt und in anderen Zusammenhängen für oder gegen ihn verwendet.[94] Demzufolge scheint es unmöglich sich gegen unerlaubte Aufnahmen erfolgreich zu wehren.[95]

In direktem Zusammenhang mit der mangelnden Transparenz steht die erhöhte Missbrauchsgefahr. Es ist nicht auszuschließen, dass Google Glass wie ein Smartphone mit inoffizieller Software bespielt oder sogar durch Dritte kontrolliert werden könnte.[96] Google verbietet zwar die rechtswidrige Nutzung seiner Datenbrille und behält sich die Abschaltung des Displays beim Aufnahmevorgang sowie die Fernabschaltung des Geräts bei Zuwiderhandlung vor.[97] Jedoch bleibt es nach wie vor ungewiss, ob der Missbrauch dadurch verhindert werden kann.[98]

4.2 Qualität und Quantität erfasster Daten

Google Glass als Wearable Computer für jedermann führt zu der Annahme, dass eine enorme Masse von Daten jeglicher Art erfasst werden kann.[99] Die von Google Glass erhobenen Daten werden neue Qualitäten aufweisen und eine viel höhere Aussagekraft besitzen als bisher erhobene Daten.[100] Darunter fallen persönliche Informationen,

---

93 *Solmecke/Kocatepe*, ZD 2014, 22; *Schwenke*, K&R 2013, 685 (686).

94 *Ziegler*, c't 13/2013, 70 (71); *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 23; *Schwenke*, K&R 2013, 685 (686).

95 *Schwenke*, K&R 2013, 685 (686).

96 Wenige Tage nach Präsentation der Brille wurde Google Glass bereits gehackt; *Schwenke*, K&R 2013, 685 (686).

97 Terme of Use – Google Glass, Internetquelle; *Weiche*rt, DANA 2/2013, 53 (54).

98 *Schwenke*, K&R 2013, 685 (686).

99 *Wright/Steventon*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 18; *Roßnagel*, in: Bizer/v. Mutius/Petri/Weichert (Hrsg.), Innovativer Datenschutz, S. 335 (336); *Maurer*, Informatik-Spektrum 27/2004, 44 (48).

100 *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 91.

Verhaltensweisen und Aussagen aber auch sensitive Daten[101] wie z. B. politische Meinungen, ethnische Herkunft oder sogar Gesundheitsinformationen der Glass-Träger oder Dritter.[102] Während überwiegend Bedenken im Hinblick auf die Daten Dritter geäußert werden, dürfen die Gefahren für den Glass-Träger selbst nicht unterschätzt werden. Die Datenbrille kann ebenso eigene, geheime Daten aufnehmen, wenn z. B. am Geldautomaten die Geheimzahl eingegeben wird und diese Daten versehentlich aufgenommen werden. Diese geheimen Daten werden wie alle anderen Daten auf den Google-Servern gespeichert, das zu einer erhöhten Missbrauchsgefahr führen könnte.[103] Somit betrifft der Aspekt des Datenschutzes die Glass-Träger genauso wie betroffene Dritte.

Hinzu kommt der erhebliche quantitative Anstieg des Datenflusses, unter der Annahme, dass fast jeder, der ein Smartphone besitzt, auch Google Glass nutzen könnte.[104] Dadurch werden die Vorgänge der Erhebung und Verarbeitung personenbezogener Daten erheblich gesteigert.[105] Weiter könnte der Einsatz von Google Glass zu persönlichen Überwachungs- und Beweissicherungszwecken im privaten, wie auch geschäftlichen Bereich ansteigen und sich aufgrund fehlender Transparenz negativ zu Lasten der Betroffenen auswirken.[106]

4.3 Mangelnde Vorhersehbarkeit künftiger Nutzung

Die von Google Glass erfassten Informationen werden auf Google-Servern gespeichert, um sie mit anderen Nutzern und Diensten zu teilen.[107] Dadurch fehlt es an der entsprechenden Kontrolle und Vorher-

---

101 Siehe dazu *Tinnefeld*, in: Roßnagel, Hdb DS, 4.1 Rn. 36 ff.
102 *Schwenke*, K&R 2013, 685 (686).
103 *Solmecke/Kocatepe*, DuD 2014, 22 (24).
104 *Schwenke*, K&R 2013, 685 (686); ebenso dazu *v. Stechow*, Datenschutz durch Technik, S. 57 ff.
105 *Roßnagel/Müller*, CR 2004, 625 (628).
106 *Schwenke*, K&R 2013, 685 (686); siehe dazu der Einsatz von „Dash Cams" für Beweiszwecke in Autos, Überblick über aktuelle Lage *Lachenmann/Schwiering*, NZV 2014, 291.
107 *Solmecke/Kocatepe*, ZD 2014, 22 (23); *Schenke*, K&R 2013, 685 (686).

sehbarkeit der künftigen Nutzung, woraus die Gefahr der ungewollten Datenpreisgabe resultiert.[108] Ferner verbietet Google in den Entwicklerrichtlinien die Gesichts- und Spracherkennung, jedoch mit der Einschränkung, dass dies „derzeit" gilt.[109] Ein völliger Ausschluss dieser Funktion ist folglich nicht gewährleistet.

Durch die von Google Glass erfassten Daten könnten sehr feingranulare Profile über die Handlungen, Bewegungen, sozialen Beziehungen, Verhaltensweisen, Einstellungen und Präferenzen von den Betroffenen erzeugt werden.[110] Solche Nutzerprofile hätten das Potenzial, sowohl Konsumverhalten, wie auch die politische Gesinnung durch Kontrolle des Informationsflusses zu steuern.[111] Insbesondere durch die zwingende Anlegung eines Google-Kontos, um viele weitere Google-Angebote in voller Funktionalität nutzen zu können, ist es für das Unternehmen leicht personenbezogene Daten aus einem Dienst mit Informationen und Daten aus anderen Google-Diensten zu verknüpfen.[112] Zudem könnten auf Basis der GPS-Daten, die die Datenbrille auf die Google-Server übermittelt, und deren Verknüpfung mit weiteren Daten, die Bewegungen einer Person in Form eines Bewegungsprofils nachvollzogen werden.[113] Kombiniert Google nun diese Profile mit weiteren auf den Google-Servern gespeicherten Daten wie z. B. den Kameraaufnahmen, eröffnet sich der Weg zu einer völligen Google-Überwachung.[114] Letztlich besteht immer die Möglichkeit, die

---

108 *Ziegler*, c't 13/2013, 70 (71); siehe zur Möglichkeit der Gesichtserkennung, *Karg*, HFR 2012, 120 (123 f.).

109 Zur Gesichtserkennungsfunktion von Google Glass, Internetquelle.

110 *Roßnagel*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 265 (272); *Friedewald/Lindner*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 207 (208).

111 *Schwenke*, K&R 2013, 685 (686); *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 96; zu Gefahren von Datensammlungen *v. Stechow*, Datenschutz durch Technik, S. 58 f.

112 *Becker/Becker*, MMR 2012, 351.

113 *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 96 f.; *Solmecke/Kocatepe*, ZD 2014, 22 (24).

114 *Claußß*, Die Welt v. 25.01.2015; *Solmecke/Kocatepe*, ZD 2014, 22 (24); *Wright/Stevenson*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 17 (34).

qualitativ hochwertigen von Google Glass erfassten Daten und Profile zu unerwünschten Zwecken zu nutzen.[115]

Gleichwohl bestehen im Hinblick auf den NSA-Überwachungsskandal Zweifel gegenüber staatlichen Zugriffen, die vorliegende Datensammlungen für geheimdienstliche oder ordnungsrechtliche Zwecke einsetzen.[116] Speziell nach Bekanntwerden, dass der Geheimdienst NSA mit dem Programm Prism auch auf Server von Google zugreift und deren Nutzer überwacht.[117] Desgleichen muss in diesem Zusammenhang bedacht werden, dass Datenflüsse nicht durch staatliche Grenzen beschränkt sind und damit eine Vielzahl unkontrollierbarer und intransparenter Datenzugriffe stattfinden könnten.[118]

4.4 Folgerung

Insgesamt gehen von Google Glass enorme rechtliche Gefahren aus, die gleichzeitig ein gewaltiges Eingriffspotenzial in die Rechtsgüter Dritter und des Glass-Trägers selbst darstellen. Inwiefern Google Glass dabei eine Herausforderung für das deutsche Datenschutzrecht darstellen könnte, ist in den folgenden Kapiteln zu untersuchen. Dazu wird geprüft, wie die Vorschriften des Bundesdatenschutzgesetzes (BDSG) der Datenbrille entsprechend begegnen können und wie die Eingriffe in das allgemeine Persönlichkeitsrecht, insbesondere des Rechts auf informationelle Selbstbestimmung, datenschutzrechtlich zu bewerten sind.

---

115 *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 97.

116 *Friedewald/Lindner*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 207 (224); *Solmecke/Kocatepe*, ZD 2014, 22 (24); *Schwenke*, K&R 2013, 685 (686).

117 *Biermann/Pilath*, Zeit-Online v. 07.06.2013.

118 *Schwenke*, K&R 2013, 685 (686); *Janisch/Prantl*, Süddeutsche.de v. 06.07.2013.

5 Grundlagen des Datenschutzrechts

Die datenschutzrechtlichen Anforderungen an Google Glass finden sich auf unterschiedlichen normativen Ebenen. Grundlage der Analyse bildet das deutsche Verfassungs- und Datenschutzrecht. Bevor primär auf die datenschutzrechtliche Bewertung von Google Glass eingegangen wird, sind vorab die hierfür relevanten rechtlichen Grundlagen zu erläutern. Die normativen Vorgaben des Datenschutzrechts bestehen sowohl auf internationaler als auch auf europäischer und nationaler Ebene. Aufgrund des begrenzten Ausmaßes dieser Arbeit wird ausschließlich auf die entsprechenden Grundlagen des Europarats, der Grundrechte Charta der Europäischen Union (GRC) sowie auf die EG-Datenschutzrichtlinie 95/46/EG (DSRL) eingegangen. Diese völkerrechtlichen und europäischen Grundlagen können, insbesondere in diesem aktuellen Fall, in Bezug auf das Vorlageverfahren vor dem Europäischen Gerichtshof (EuGH) gem. Art. 267 AEUV Bedeutung erlangen. Anschließend werden die durch Google Glass gefährdeten nationalen Grundrechte und die Ausgestaltung der Eingriffe thematisiert.

5.1 Europarat

Die am 4.11.1950 von den Mitgliedstaaten des Europarats unterzeichnete Europäische Menschenrechtskonvention[119] (EMRK) enthält keinen eindeutigen Bezug zum Datenschutz.[120] Jedoch lässt sich für den Datenschutz, das Recht jeder Person „auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“ gemäß Art. 8 Abs. 1 EMRK heranziehen.[121] Dieser Artikel schützt das Recht

[119] Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 04.11.1950, in Deutschland ratifiziert am 07.08.1952, BGBl. 1952 II, 685.

[120] *Simitis*, in: Simitis, Einleitung: Geschichte – Ziele – Prinzipien, Rn. 151.

[121] Z. B. EGMR NJW 2011, 1333; Der Schutz des Privatlebens übernimmt Funktionen des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und somit insbesondere auch auf das Recht auf informationelle Selbstbestimmung siehe dazu Kapitel 5.3.1.

auf Identität und Entwicklung der Person.[122] Danach soll eine Person in einer geschützten Sphäre ihr Leben nach ihrer Wahl leben und ihre Persönlichkeit frei entwickeln.[123] Davon erfasst ist auch die Möglichkeit, Beziehungen zu anderen Menschen, auch sexueller Art, aufzunehmen.[124] Obwohl dieser Artikel keine ausdrückliche Garantie des Rechts auf Schutz personenbezogener Daten enthält, wird der Datenschutz nach ständiger Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) als ein spezifisch ausgestalteter Teilbereich des Rechts auf Achtung der Privatsphäre angesehen.[125] Der Schutzbereich von Art. 8 Abs. 1 EMRK ist somit eröffnet, wenn Daten eines Grundrechtsträgers erhoben, gespeichert oder verarbeitet werden und dieser dadurch in seinem Privatleben beeinträchtigt ist.[126]

Hinsichtlich des Rechts der Europäischen Union (EU) nimmt die EMRK ebenfalls eine herausragende Stellung ein. Schon der EuGH berücksichtigte zur Auslegung des Gemeinschaftsrechts die Vorgaben der EMRK zusammen mit den Verfassungsüberlieferungen der Mitgliedstaaten als Rechtserkenntnisquelle europäischer Grundrechte.[127] Auch zur Auslegung und Prüfung des Europäischen Datenschutzrechts, im Besonderen der DSRL, hat sich der EuGH auf die EMRK berufen und konkret anhand Art. 8 EMRK geurteilt.[128] Seit dem Vertrag von Lissabon rückt die GRC als verbindliches Primärrecht in den Fokus des Europäischen Grundrechtsschutzes. Die Vorgaben der EMRK sind aber nach Art. 6 Abs. 3 EUV als sogenannte „allgemeine Grunds-

122 Siehe dazu EGMR NVwZ 2003, 1496 = NJW 2003, 2145 = EuGRZ 2003, 584.

123 *Meyer-Ladewig*, Art. 8 EMRK, Rn. 7; *Grabenwarter*, EMRK, § 22, Rn. 6; *Frowein*, in: Frowein/Peukert, Art. 8 EMRK, Rn. 3.

124 EGMR NJW 2003, 1971; *Meyer-Ladewig*, Art. 8 EMRK, Rn. 7, 8; *Uerpmann-Wittzack*, in: Ehlers, § 3, I 1 Rn. 5.

125 EGMR, Urteil v. 6.9.1978, 5029/21; EGMR, Urteil v. 2.8.1984, 8691/79; EGMR, Urteil v. 26.3.1987, 9248/81; hierzu auch *Grabenwarter*, EMRK, § 22, Rn. 10; *Meyer-Ladewig*, Art. 8 EMRK, Rn. 40 ff.; *Schweizer*, DuD 2009, 462 ff.

126 *Grabenwarter*, EMRK, § 22, Rn. 10.

127 *Kingreen*, in: Calliess/Ruffert, Art. 6 EUV, Rn. 19; *Hatje*, in: Schwarze/Becker/Hatje/Schoo, Art. 6 EUV, Rn. 1, 16.

128 Z. B. EuGH, Slg. 2003, I-4989, Rn. 73 ff.

ätze“ Teil des Unionsrechts. Nach Art. 6 Abs. 2 EUV setzt sich die EU sogar selbst zum Ziel, der EMRK beizutreten.[129]

5.2 Unionsrecht

Mit dem am 1.12.2009 in Kraft getretenen Reformvertrag von Lissabon erlangte die GRC volle Rechtsverbindlichkeit.[130] Seither kann sich jedermann grundsätzlich vor allen Gerichten in der EU auf die Charta berufen – allerdings nur, soweit sie nach Art. 51 Abs. 1 GRC überhaupt anwendbar ist.[131] Danach gilt die Charta für die EU und für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union unter Wahrung des Subsidiaritätsprinzips. Demnach tritt die GRC erst in Geltung, soweit mitgliedstaatliche Grundrechte keinen hinreichenden Schutz gewähren. Demgemäß können Unionsorgane Sekundärrecht für Mitgliedstaaten erst an der GRC ausrichten, wenn mitgliedstaatliches Recht unzureichend schützt.[132] Mit Art. 6 Abs. 1 EUV wird die GRC offiziell anerkannt und mit den Verträgen gleichgestellt. Die GRC ist damit Teil des Primärrechts der EU.[133]

Entscheidend für den Datenschutz sind Art. 8 und Art. 7 der GRC. Aus den Erläuterungen der GRC geht hervor, dass die Rechte aus Art. 7 GRC und damit auch die Achtung des Privatlebens den Rechten entsprechen, die durch die (wörtlich wiedergegebene) Vorschrift des Art. 8 EMRK garantiert werden.[134] Daher haben sie gem. Art. 52 Abs. 3 S. 1 GRC grundsätzlich die gleiche Bedeutung und Tragweite wie die Konventionsrechte.[135] Der EuGH hat dies sowohl in

---

129 *Kingreen*, in: Calliess/Ruffert, Art. 6 EUV, Rn. 19.

130 *Classen/Nettesheim*, in: Oppermann/Classen/Nettesheim, Europarecht, § 17, Rn. 8; *Hilf/Schorkopf*, in: Grabitz/Hilf, Art. 6 EUV, Rn. 67; *Hatje*, in: Schwarze/Becker/Hatja/Schoo, Art. 6 EUV, Rn. 5.

131 Siehe dazu *Jarass,* Art. 51 GRC, Rn. 2 ff.

132 *Kirchhof*, NJW 2011, 3681 (3685).

133 *Kingreen*, in: Calliess/Ruffert, Art. 6 EUV, Rn. 8; *Hatje*, in: Schwarze/Becker/Hatje/Schoo, Art. 6 EUV, Rn. 6.

134 *Jarass*, Art. 7 GRC, Rn. 2; *Bernsdorff*, in: Meyer, Art. 7 GRC, Rn. 14.

135 Charta-Erläuterungen, ABl. 2007 C 303/20, 33; zu der Bedeutung des Datenschutzes siehe Kap. 5.1.

der Gewährleistungs- als auch in der Rechtfertigungsdimension für Art. 7 und Art. 8 GRC im Hinblick auf Art. 8 EMRK betont.[136] Das Recht auf Achtung des Privatlebens umfasst auch den Bereich des informationellen Selbstbestimmungsrechts[137] und steht dadurch in enger Verbindung zu Art. 8 GRC der gleichzeitig lex specialis zu Art. 7 GRC ist.[138]

Nach Art. 8 GRC hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat überdies das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschrift wird von einer unabhängigen Stelle überwacht. Mit diesem Artikel wird das Recht auf Schutz personenbezogener Daten in den Rang eines Grundrechts auf primärrechtlicher Ebene erhoben.[139] Art. 8 GRC soll sich als „innovatives" Grundrecht[140] den Herausforderungen der heutigen und künftigen Entwicklungen in der Informationstechnologie stellen.[141]

Diese Vorschrift „stützt" sich u. a. auf die DSRL,[142] sodass auch deren Konzept, den Datenschutz des Einzelnen durch die Beseitigung von Hemmnissen für den freien Datenverkehr in der Gemeinschaft zu ver-

136 EuGH, Urteil v. 9.11.2010, C-92-09 u. C-93-09.

137 Vgl. die Begründungen zu Art. 8 CONVENT 5 und Art. 19 CONVENT 28 sowie die Änderungsanträge (CONVENT 35) von Friedrich (D) und Korhals Altes (NL) zu Art. 19 CONVENT 28.

138 *Bernsdorff*, in: Meyer, Art. 8 GRC, Rn. 13; *Kingreen*, in: Calliess/Ruffert, Art. 8 GRC, Rn. 1.

139 *Hatje*, in: Schwarze/Becker/Hatje/Schoo, Art. 6 EUV, Rn. 6; *Bernsdorff*, in: Meyer, Art. 8 GRC, Rn. 1; *Kingreen*, in: Calliess/Ruffert, Art. 6 EUV, Rn. 8.

140 *Bernsdorff*, in: Meyer, Art. 8 GRC, Rn. 12.

141 Mitteilung der Kommission zum Status der Grundrechtscharta der Europäischen Union vom 11.10.2000, KOM (2000) 644 endg.

142 Konvent der Charta der Grundrechte der Europäischen Union, Erläuterungen zur Charta der Grundrechte der Europäischen Union, ABl. C 303 vom 14.12.2007, 20.

bessern, übernommen wird.[143] Somit bestimmen sich Umfang und Grenzen des Grundrechts nach Maßgabe der vorhandenen (sekundärrechtlichen) Regelungen.[144] Zudem stellt die DSRL die wichtigste Regelung im Sekundärrecht dar. Sie erzeugt in den Mitgliedstaaten Datenschutzmindeststandards und damit zugleich ein einheitliches Basisniveau für den Datenschutz.[145] Für datenschutzrechtlich relevante Sachverhalte hat die Richtlinie als Auslegungshilfe Bedeutung, soweit nationale Vorschriften nicht eindeutig sind. Behörden und Gerichte sind nach der EuGH-Rechtsprechung zudem zur richtlinienkonformen Auslegung verpflichtet.[146]

5.3 Deutscher Grundrechtsschutz

Das deutsche Datenschutzrecht ist zum Teil durch die genannten völker- und europarechtlichen Vorgaben geprägt worden und hat zugleich deren Entwicklung beeinflusst.[147] Im Gegensatz zur GRC ist im Grundgesetz ein Grundrecht auf Datenschutz nicht ausdrücklich normiert. Allerdings hat das Bundesverfassungsgericht (BVerfG) in langjähriger Rechtsprechung aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG[148] grundrechtliche Gewährleistung zum Schutz Betroffener beim Umgang mit ihren personenbezogenen Daten abgeleitet. Wie oben bereits erläutert sind Art. 8 EMRK sowie Art. 8 GRC dabei von besonderer Bedeutung, da diese den Schutzmaßstab für das allgemeine Persönlichkeitsrecht vorgeben.[149] Grundsätzlich soll vor Beeinträchtigungen der engeren persönlichen Lebenssphäre, die Selbstbestimmung und die Grundbedin-

---

143 Erwägungsgründe Nr. 8 und 9 der Richtlinie 95/46/EG, siehe im Einzelnen *Brühann*, EuZW 2009, 639 ff.; *Bernsdorff*, in: Meyer, Art. 8 GRC, Rn. 15.

144 *Bernsdorff*, in: Meyer, Art. 8 EMRK, Rn. 14; *Kingreen*, in: Calliess/Ruffert, Art. 8 GRC, Rn. 6.

145 *Weichert*, in: Kilian/Heussen, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, Rn. 20; *Hornung*, Die digitale Identität, S. 137.

146 EuGH, Slg. 1984, I-1891.

147 *Hornung*, Die digitale Identität, S. 138.

148 BVerfGE 6, 32.

149 *Polenz*, in: Kilian/Heussen, Teil 13 I, Rn. 1.

gungen der Persönlichkeitsentfaltung bewahrt werden.[150] Bei der Nutzung von Google Glass muss das allgemeine Persönlichkeitsrecht und insbesondere seine Konkretisierungen in dem Recht auf informationelle Selbstbestimmung, dem Recht am eigenen Bild und dem Recht am eigenen Wort beachtet werden. Demzufolge bietet es sich im Folgenden an diese einschlägigen Grundrechte zu erläutern.

5.3.1 Das Recht auf informationelle Selbstbestimmung

Grundsätzlich ist zwischen den verfassungsrechtlichen Anforderungen und einfachgesetzlichen Datenschutznormen zu unterscheiden, die allerdings häufig Ausprägungen des Verfassungsrechts wiederspiegeln.[151] Prägend für das Datenschutzrecht ist das (Grund-) Recht auf informationelle Selbstbestimmung,[152] das das BVerfG in seinem Volkszählungsurteil aus dem allgemeinen Persönlichkeitsrecht entwickelte. Demzufolge ist es „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[153] Der Einzelne soll dadurch in die Lage versetzt werden, selbstbestimmt entscheiden zu können, welche Daten und damit welches Bild dieser von sich selbst preisgeben und darstellen will. Wer nämlich „nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden".[154] Nach der Rechtsprechung gibt es aufgrund der technischen Möglichkeiten „kein belangloses Datum"[155] mehr. Demzufolge ist die traditionelle Sphärentheorie[156]

---

150 *Di Fabio*, in: Maunz/Düring, Art. 2 GG, Rn. 147.
151 *Hornung*, Die digitale Identität, S. 138.
152 Von Bedeutung ist, dass das BVerfG von einem Grundrecht spricht siehe dazu BVerfGE 84, 239, 280.
153 BVerfGE 65, 1.
154 BVerfGE 65, 1 (43).
155 BVerfGE 65, 1 (45).
156 Siehe dazu *Lang*, in: Epping/Hillgruber, Art. 2 GG, Rn. 35 ff.

des allgemeinen Persönlichkeitsrechts nicht ausreichend, da aufgrund der Informationstechnologie auch eine für sich unerhebliche Information in Verknüpfung mit anderen Daten Rückschlüsse auf den Betroffenen, seinen Lebensweg und seine Persönlichkeit zulassen kann.[157] Der Grad der Persönlichkeitsrelevanz ist somit für die Eröffnung des Schutzbereichs irrelevant, sodass auch nicht nach Intim-, Privat- und Individualsphäre getrennt wird.[158]

Dennoch ist das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet. Alle Einschränkungen dieses Rechts müssen dem Schutze und der Förderung von Gemeinschaftsgütern dienen und insbesondere zu diesen Zwecken geeignet, erforderlich und verhältnismäßig im engeren Sinne sein. Weiter bedürfen diese Einschränkungen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar, und für den Bürger erkennbar ergeben, und damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht.[159]

Während sich die dem Volkszählungsurteil zugrundeliegende Verfassungsbeschwerde gegen eine staatliche Maßnahme richtete, hat der Schutz der informationellen Selbstbestimmung mittlerweile vor allem gegenüber Privaten Bedeutung erlangt.[160] Das Recht auf informationelle Selbstbestimmung entfaltet als objektive Norm seinen Rechtsgehalt auch im Privatrecht und strahlt dementsprechend auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus.[161] Das Fortschreiten der Technik und daraus resultierende neuartige Gefähr-

---

157 *Kunig*, in: Münch/Kunig, Art. 2 GG, Rn. 41; *Hufen*, Staatsrecht II, § 3, Rn. 4; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 62.

158 Siehe z. B. BVerfGE 96, 171 (181).

159 *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Hopfau, Art. 2 I GG, Rn. 26; *Polenz,* in: Kilian/Heussen, Teil 13 II, Rn. 10; *Hufen*, Staatsrecht II, § 3, Rn. 12; *Starck*, in: v. Mangoldt/Klein/Starck, Art. 2 Abs. 1 GG, Rn. 115.

160 *Kunig*, in: Münch/Kunig, Art. 2 GG, Rn. 38.

161 BVerfGE 7, 198; BVerfG, NJW 1991, 2411; vgl. auch *Roßnagel/Schnabel*, NJW 2008, 3534 ff.; hierzu *Roßnagel/Pfitzmann/Garstka,* Modernisierung des Datenschutzrechts, S. 47; grundlegend BVerfGE 7, 198 (205); für das Recht auf informationelle Selbstbestimmung BVerfGE 84, 192 (194 f.); *Dreier,* in: Dreier, Art. 2 I GG, Rn. 97; *Kunig*, in: Münch/Kunig, Art. 2 GG, Rn. 40.

dungslagen sind damit nur selten staatlichem Handeln geschuldet.[162] Nicht zuletzt deshalb, da Techniken wie Google Glass primär für den privaten Gebrauch bestimmt sind.

Das Recht auf informationelle Selbstbestimmung erlangt bei der Nutzung von Google Glass besondere Relevanz. Jede Verwendung personenbezogener Daten durch Google Glass stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG dar. Gerade durch die intransparente Erfassung der persönlichen Daten, ist es dem Einzelnen nicht möglich zu bestimmen, welche Daten über ihn veröffentlicht oder verwendet werden. Dabei ist es besonders problematisch, dass Aufnahmen wie Bilder oder Gespräche ebenso wie alle anderen Daten automatisch auf dem Server des Unternehmens Google gespeichert werden. Ein noch tieferer Eingriff in das Recht auf informationelle Selbstbestimmung liegt vor, soweit die auf den Google-Servern gespeicherten Daten mit vorhandenen Informationen aus einem anderen Google Dienst oder Diensten von Drittanbietern abgeglichen oder kombiniert werden können.[163] Hinzu kommt, dass es sich bei Bildinformationen aufgrund der hohen Informationsdichte zu den intensivsten Formen der Erhebung personenbezogener Daten handelt.[164]

5.3.2 Das Recht am eigenen Bild

Als weitere Ausprägung des allgemeinen Persönlichkeitsrechts und gleichzeitige Konkretisierung des Rechts auf informationelle Selbstbestimmung ist das Recht am eigenen Bild zu sehen.[165] Dieses Recht schützt die optische Perspektive der Selbstdarstellung in der Öffentlichkeit. Der Einzelne wird vor Aufnahmen seines Abbildes durch Fo-

[162] Zu berücksichtigen ist jedoch, dass sich der Staat manchmal solche Techniken zu eigen macht, z. B. im Fall der Vorratsdatenspeicherung, Onlinedurchsuchung mittels staatlicher Trojaner-Software, bei der sich der Staat den Methoden von Cyberkriminellen bedient.

[163] *Solmecke/Kocatepe*, ZD 2014, 22 (23); *Erd*, NVwZ 2011, 19 (21).

[164] *v. Zezschwitz*, in: Roßnagel, Hdb DS, 9.3, Rn. 7.

[165] *Kunig*, in: Münch/Kunig, Art. 2 GG, Rn. 38.

tografie und Film sowie deren Darbietung, Verbreitung oder sonstiger Verwertung geschützt, soweit dies ohne oder gegen seinen Willen stattfindet.[166] Dadurch soll eine Einfluss- und Entscheidungsmöglichkeit hinsichtlich der Gestattung von Anfertigung und Verwendung von Fotografien und ähnlichen bildlichen Aufzeichnungen seiner Person durch andere gewährleistet werden.[167]

Einzelne Gehalte des Rechts am eigenen Bild haben eine gesetzliche Regelung im §§ 22, 23 Kunsturhebergesetz (KUG) gefunden.[168] Gem. § 22 S. 1 KUG ist die Verbreitung und öffentliche Zurschaustellung von Bildnissen grundsätzlich nicht ohne Einwilligung des Abgebildeten zulässig. Unter die öffentliche Zurschaustellung fällt z. B. das Teilen von Bildern in einem sozialen Netzwerk.[169] Ausnahmen der in § 22 KUG geforderten Einwilligung normiert der in § 23 Abs. 1 KUG geregelte Katalog abschließend. Allerdings ist die Rückausnahme nach § 23 Abs. 2 KUG zu beachten, wonach die Ausnahmen von der Einwilligungserfordernis wiederum nicht gelten. Danach ist eine Verbreitung und öffentliche Zurschaustellung eines Bildnisses trotz des Vorliegens eines Ausnahmetatbestandes nach § 23 Abs. 1 KUG unzulässig, soweit eine Verletzung berechtigter Interessen vorliegt. Damit sind insbesondere Fälle der Verletzungen der Privat- und Intimsphäre, Verfälschungen des Aussagegehalts oder eine wirtschaftliche Ausbeutung erfasst.[170] Um dies beurteilen zu können, bedarf es einer umfassenden Abwägung der widerstreitenden Interessen im Einzelfall.[171]

Die Herstellung eines Bildnisses ohne Zustimmung der betroffenen Person fällt nicht unter das KUG, stellt aber ggf. eine Verletzung des

166 BVerfGE 34, 238 (245 f.); BVerfGE 54, 148 (154).
167 BVerfGE 101, 361 (381).
168 *Dreier*, in: Dreier, Art. 2 I GG, Rn. 73.
169 Siehe dazu die Ausführungen von *Schwenke*, K&R 2013, 685 (687).
170 *Fricke*, in: Wandtke/Bullinger, § 23 KUG, Rn. 29-40; *Dreier/Specht*, in: Dreier/Schulze, § 23 KUG, Rn. 48.
171 EGMR GRUR 2004, 1051; *Fricke*, in: Wandtke/Bullinger, § 23 KUG, Rn. 28 f; *Dreier/Specht*, in: Dreier/Schulze, § 23 KUG, Rn. 46.

allgemeinen Persönlichkeitsrechts dar.[172] An dieser Stelle befindet sich die Verbindung zum Datenschutzrecht, da der Anwendungsbereich des BDSG nach § 1 Abs. 2 BDSG auch die Erhebung von personenbezogenen Daten[173] umfasst.[174] Somit unterfällt das Anfertigen von Bildern dem BDSG und seine weitere Nutzung, zumindest in Form der Veröffentlichung, dem KUG.[175]

Durch Google Glass ist es für die Nutzer besonders einfach Aufnahmen von Personen mit wenigen Schritten Dritten zugänglich zu machen.[176] Allerdings muss niemand die unbefugte Anfertigung und Verbreitung seiner Bildnisse dulden. Dahingehend ist die Rechtslage bei Google Glass keine andere als bei herkömmlichen Aufnahmegeräten.[177] Aufgrund der ständigen Verbindung zum Internet liegen solche Zurschaustellungen insbesondere dann vor, wenn Glass-Träger die Aufnahmen innerhalb von sozialen Netzwerken einstellen und allen Nutzern des sozialen Netzwerks zugänglich machen. Somit könnte von einer Beeinträchtigung des Rechts am eigenen Bild gem. § 22 S. 1 KUG ausgegangen werden.

5.3.3 Das Recht am eigenen Wort

In akustischer Perspektive schützt das Recht am eigenen Wort die Selbstentfaltung in Form der „Selbstbestimmung über die Adressierung des Gesprächs".[178] Demgemäß wird die Freiheit des Grundrechtsrechtsträgers geschützt, durch die Wahl zwischen öffentlicher oder vertraulicher Äußerung festzulegen, wem gegenüber er sich darstellt.[179] Es bleibt jedem selbst überlassen zu entscheiden, ob der Inhalt

---

172 BGHZ 24, 200 (208) = NJW 1957, 1315; BGH, NJW 1966, 2353; BGHZ 80, 25 = NJW 1981, 1089; *Dreier/Specht*, in: Dreier/Schulze, § 22 KUG, Rn. 12; *Fricke*, in: Wandtke/Bullinger, § 22 KUG, Rn. 9.

173 Bilder sind personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG siehe dazu *Gola/Schomerus*, § 3 BDSG, Rn. 2 ff.

174 *Schnabel*, ZUM 2008, 657 (661).

175 *Schnabel*, ZUM 2008, 657 (662).

176 *Tung*, ZDnet v. 17.05.2013.

177 *Solmecke/Kocatepe*, ZD 2014, 22.

178 BVerfGE 106,28 (44).

179 BVerfGE 34, 238 (246); BVerfGE 54, 208 (217); BVerfGE 82, 236 (269).

eines Gesprächs oder Schriftstücks ausschließlich dem Gesprächspartner bzw. Adressaten, einem bestimmten Personenkreis oder der Öffentlichkeit zugänglich sein soll. Vom Schutzbereich umfasst ist das nicht-öffentliche Wort.[180]

Wird Google Glass dazu genutzt nicht-öffentliche Tonaufnahmen ohne das Einverständnis des Betroffenen anzufertigen und diese Aufnahmen dann gegen den Willen des Aufgezeichneten gegenüber Dritten abzuspielen oder im Internet zu verbreiten, stellt dies eine Verletzung des verfassungsrechtlich geschützten Rechts am eigenen Wort dar.[181] Gleichwohl kommen im Hinblick auf die in Art. 5 Abs. 1 GG gewährte Meinungsfreiheit Bedenken auf. Die Meinungsfreiheit umfasst auch das Recht, keine Meinung bilden zu müssen, seine Meinung nicht äußern zu müssen und seine Meinung nicht verbreiten zu müssen.[182] Insofern ist davon auszugehen, dass jeder Mensch stets mit der Aufnahme des von ihm Gesprochenen rechnen muss, wenn Google Glass von zahlreichen Personen genutzt wird. Dies könnte zur Folge haben, dass die Menschen sich in Zukunft nicht mehr trauen ihre Meinung frei zu äußern, soweit Glass-Träger sich in ihrem Umfeld aufhalten.[183] Somit könnte eine Beeinträchtigung des Rechts am eigenen Wort gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG vorliegen.

---

180 BVerfG NJW 1980, 2070; BVerfGE NJW 1992, 815; BGH NJW 1981, 1089; *Dreier*, in: Dreier, Art. 2 I GG, Rn. 74; *Nink*, in: Spindler/Schuster, § 823 BGB, Rn. 30.

181 BGHZ 13, 334; BGHZ 15, 249; *Solmecke/Kocatepe*, ZD 2014, 22 (23).

182 BVerfGE 65, 1 (40 f.); *Grabenwarter*, in: Maunz/Düring, Art. 5 GG, Rn. 95; *Wendt*, in: Münch/Kunig, Art. 5 GG, Rn. 18.

183 *Solmecke/Kocatepe*, ZD 2014, 22 (24).

6 Datenschutzrechtliche Bewertung

Wie vorab festgestellt, ist jede Verwendung personenbezogener Daten ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung.[184] Die Nutzung von Google Glass beeinträchtigt in jedem Fall die freie Entfaltung der Persönlichkeit der Betroffenen, unabhängig davon, ob sich Glass-Träger in der Öffentlichkeit bewegen, Fotos bzw. Videos machen, Informationen über Dritte im Internet teilen oder sogar das Verhalten einzelner Personen analysieren und auswerten. Schließlich verursacht die Verarbeitung der personenbezogenen Daten durch Google Glass vielfältige Risiken für die informationelle Selbstbestimmung sowie die zu seiner Gewährleistung entwickelten Grundsätze des Datenschutzrechts.[185] Eine solche Beeinträchtigung des Persönlichkeitsrechts der Betroffenen ist nur zulässig, wenn sich gesetzliche Rechtfertigungsgründe oder ein besonderes Interesse der Betroffenen dafür finden lassen. Im Hinblick auf die zahlreichen datenschutzrechtlichen Bedenken ist zu prüfen, ob das deutsche Datenschutzrecht Regelungen enthält, die geeignet sind, die in Kapitel 3 erläuterten Szenarien zu legitimieren.

6.1 Anwendbarkeit des Datenschutzrechts

Nach § 1 Abs. 1 BDSG dient das BDSG dem Schutz natürlicher Personen vor den Gefahren der Datenverarbeitung für ihr Persönlichkeitsrecht. Normadressaten sind gem. § 1 Abs. 2 Nr. 1 und 2 BDSG öffentliche Stellen des Bundes sowie in Ausnahmefällen auch öffentliche Stellen der Länder, soweit sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt. Ebenso fallen wie in diesem Fall nicht-öffentliche

---

184 S. BVerfGE 100, 313 (366); dies gilt auch für die Datenverwendung durch private Stellen s. BVerfGE 84, 192, (195).

185 *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 85; *Roßnagel/Müller*, CR 2004, 625; zu den datenschutzrechtlichen Prinzipien gehören die Zweckfestlegung und Zweckbindung, Erforderlichkeit, Datenvermeidung und Datensparsamkeit, Transparenz, Unabhängige Kontrollen, Technischer Schutz, Rechte der Betroffenen.

Stellen gem. § 1 Abs. 2 Nr. 3 BDSG in den Anwendungsbereich des BDSG, jedoch nur soweit der Datenumgang nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Nach § 1 Abs. 3 S. 1 BDSG gilt das BDSG nur subsidiär, es kommt als Auffanggesetz immer dann zur Anwendung, wenn keine speziellere Rechtsvorschrift einschlägig ist.[186]

Der Anwendungsbereich ist gem. § 1 Abs. 2 BDSG nur im Fall des Umgangs mit personenbezogenen Daten eröffnet. Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Insofern handelt es sich bei den von Google Glass erfassten Personenabbildungen und weiteren Daten wie Adressen, Namen oder Lokalisierungsdaten um personenbezogene Daten i. S. d. § 3 Abs. 1 BDSG.[187]

6.1.1 Persönlicher oder familiärer Umgang mit personenbezogenen Daten

Zunächst ist zu prüfen, ob es sich bei den von Google Glass erfassten Daten ausschließlich um eine persönliche oder familiäre Nutzung handelt und somit die Anwendbarkeit des BDSG von vornherein gem. § 1 Abs. 2 Nr. 3 BDSG auszuschließen ist.[188]

Mit „ausschließlich für persönliche oder familiäre Tätigkeiten" grenzt das Gesetz den Bereich der persönlichen Lebensführung von der beruflichen und geschäftlichen Sphäre ab.[189] Maßgeblich ist, ob Daten

---

[186] *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 1 BDSG, Rn. 12 ff.; *Plath*, in: Plath, § 1 BDSG, Rn. 35 ff.; *Dix*, in: Simitis, § 1 BDSG, Rn. 158.

[187] So auch EuGH, BeckRS 2014, 82595, Rn. 22; *Dammann*, in: Simitis, § 3 BDSG, Rn. 4 ff.; *Gola/Schomerus*, § 3 BDSG, Rn. 2 ff.; siehe auch *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 61; *Tinnefeld*, in: Roßnagel, Hdb DS, 4.1, Rn. 18; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 3 BDSG, Rn. 19, 21a.

[188] Parallel zu der Reglung in § 1 Abs. 2 Nr. 3 BDSG gelten die in den §§ 27-32 BDSG geregelten Rechtsgrundlagen der Datenverarbeitung gem. § 27 Abs. 2 S. 1 BDSG nicht, wenn der Umgang mit den personenbezogenen Daten ausschließlich für persönliche oder familiäre Zwecke erfolgt.

[189] *Dammann*, in: Simitis, § 1 BDSG, Rn. 149.

ausschließlich im Rahmen des persönlichen Konsums, der Freizeit oder der rein sozialen und familiären Kontakte genutzt werden. Diese Form der Datenverarbeitung umfasst z. B. Adressen von Freunden oder die Kommunikation mit diesen.[190] Familiäre Tätigkeiten beziehen sich auf die Rolle des Einzelnen i. R. d. Familie wie etwa der Kontakt mit Verwandten.[191] Diese Tätigkeiten bzw. Zwecke werden unter der Annahme, dass sie keine Risiken für die Privatsphäre des Einzelnen mit sich bringen, da die Datenverarbeitung lediglich im eigenen häuslichen Bereich und nur für den eigenen Gebrauch erfolgt, aus dem Anwendungsbereich des Datenschutzrechts herausgenommen.[192] Allerdings verfällt die Privilegierung sobald jegliche nach außen gerichtete, über den persönlichen und familiären Kreis hinaustretende Tätigkeit den privilegierten Rahmen verlässt.[193]

Wird Google Glass ausschließlich im privaten und häuslichen Bereich für persönliche oder familiäre Tätigkeiten genutzt, kommt es nach der rechtlichen Auffassung zu keiner Beeinträchtigung des Persönlichkeitsrechts, sodass die Vorschriften des BDSG nicht anzuwenden sind.[194] In der Regel fällt auch die private Nutzung von Kameras ebenso die von Google Glass, unter persönliche Tätigkeiten auch wenn die Erhebung im öffentlichen Raum erfolgt.[195] Unter Berücksichtigung des umfassenden Schutzzwecks dieses Gesetzes ist die Ausnahme der Anwendbarkeit des BDSG anzuzweifeln, wenn man bedenkt, dass sich Glass-Träger in der Öffentlichkeit bewegen, dort gezielt personenbezogene Daten erfassen und diese an Google, Facebook oder anderen Diensten im Internet zu Zwecken der Verarbeitung und Nutzung weiterleiten können.[196] Infolgedessen ist diese Ausnahme im

190 *Dammann*, in: Simitis, § 1 BDSG, Rn. 151; *Plath*, in: Plath, § 1 BDSG, Rn. 31; *Schmidt*, in: Taeger/Gabel, § 1 BDSG, Rn. 31; *v. Lewinski*, in: Auernhammer, § 1 BDSG, Rn. 19

191 *Dammann*, in: Simitis, § 1 BDSG, Rn. 151; *Bergmann/Möhrle/Herb*, § 1 BDSG, Rn. 20.

192 *v. Lewinski*, in: Auernhammer, § 1 BDSG, Rn. 15.

193 *Dammann*, in: Simitis, § 1 BDSG, Rn. 149.

194 Anzumerken ist, dass es auch zu Verletzungen des Persönlichkeitsrechts von z. B. Familienmitgliedern im persönlichen und familiären Bereich kommen kann.

195 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 1 BDSG, Rn. 9.

196 *Schwenke*, K&R 2013, 685 (689); *Brühann*, DuD 2004, 201 (203).

Hinblick auf Beeinträchtigungen des Persönlichkeitsrechts durch den Umgang mit personenbezogenen Daten eng auszulegen.[197] Hinzu kommt, dass diese Ausnahmeregelung aus den 90er Jahren stammt und nicht berücksichtigt, welche Gefahren mittlerweile durch den enormen technischen Fortschritt auch von Privatpersonen für Dritte ausgehen können.[198] Immer mehr Privatpersonen sind in Blogs und sozialen Netzwerken in der Öffentlichkeit tätig, können dort öffentlich Meinungen publizieren, fremde Daten veröffentlichen und dadurch den Persönlichkeitsrechten Dritter erhebliche Schäden zufügen.[199] Viele Nutzer teilen ihre Aufnahmen zwar nur innerhalb eingegrenzter Personenkreise, wie z. B. unter individuell bestätigten „Freunden" auf der Plattform Facebook. Fraglich ist allerdings, ob es sich dabei tatsächlich um Freunde und eine persönliche Verbundenheit handelt, wenn davon auszugehen ist, dass Facebook Nutzer im Durchschnitt 342 Freunde haben.[200] In den meisten Fällen wird eine persönliche Verbundenheit nicht vorliegen, wenn die Verbindung lediglich auf kurzen Treffen, ähnlichen Interessen, digitalem Austausch von Gedanken oder mittelbaren Kontakten als Freund von Freunden beruht.[201] Zudem ist eine freundschaftliche oder familiäre Beziehung für die technische Verbindung oder Bezeichnung als „Freund" nicht notwendig.[202] Folglich ist davon auszugehen, dass ein solcher Datenzugang nicht stabil auf einen engen Familien- oder Freundeskreis begrenzt ist und die Angaben in Blogs oder sozialen Netzwerken keinen persönlich-familiären Charakter aufweisen.[203] Gleichwohl ist § 1 Abs. 2 Nr. 3 BDSG als Ausnahmevorschrift restriktiv auszule-

197 Vgl. EuGH, Urteil v. 11.12.2014 – C-212/13, Rn. 29.

198 *Schwenke*, K&R 2013, 685 (689); ähnlich wie von Medienschaffenden, die ebenfalls nicht vollständig aus dem Anwendungsbereich des BDSG herausgenommen werden.

199 *Jandt/Roßnagel*, ZD 2011, 160 (162); ebenso Art. 29-Datenschutzgruppe, WP 163, S. 8; siehe auch *Kartal- Aydemir/Krieg*, MMR 2012, 647.

200 *Nocun*, v. 03.05.2013, Internetquelle.

201 *Schapir*o, ZUM 2008, 273 (275).

202 *Schapiro*, ZUM 2008, 273 (276); siehe zu dieser Problematik *Jandt/Roßnagel*, ZD 2011, 160 (162).

203 *Dammann*, in: Simitis, § 1 BDSG, Rn. 151.

gen.[204] Soweit Zweifel entstehen, ob die Datenverarbeitung tatsächlich ausschließlich familiäre oder persönliche Aktivitäten betrifft, sind diese zu Gunsten einer Anwendbarkeit des BDSG auszuräumen.[205]

Damit handelt es sich bei der Nutzung von Google Glass außerhalb von persönlich-familiären Räumen nicht mehr um ausschließlich persönliche und familiäre Zwecke, soweit davon auszugehen ist, dass die erfassten personenbezogenen Daten umgehend im Internet verbreitet werden können.[206] Der Datenumgang erstreckt sich auf einen Bereich außerhalb der privaten Sphäre, und kann somit nicht als ausschließlich persönliche oder familiäre Tätigkeit angesehen werden kann.[207]

Um die Voraussetzungen des § 1 Abs. 2 Nr. 3 BDSG vollständig zu erfüllen, müsste der Datenumgang unter Einsatz von Datenverarbeitungsanlagen[208] oder mit nicht automatisierten Daten erfolgen.[209] Durch Google Glass werden die Daten mit einer technischen Vorrichtung erfasst und in den meisten Fällen sogar auf dem Gerät automatisch verarbeitet oder spätestens mit deren Übermittlung an den Server von Google oder anderen Anbietern.[210] Dadurch ist die für die Anwendung des BDSG erforderliche Verarbeitung oder Nutzung der Daten unter Einsatz von Datenverarbeitungsanlagen sowie deren Erhebung zu diesen Zwecken ebenfalls gegeben.[211] Folglich sind die Tatbestandsvoraussetzungen des § 1 Abs. 2 Nr. 3 BDSG erfüllt und der Anwendungsbereich des BDSG eröffnet.

---

204 *Dammann*, in: Simitis, § 1 BDSG, Rn. 148.

205 *Jandt/Roßnagel*, ZD 2011, 160 (162); *Schenk/Niemann/Reinmann/Roßnagel*, Digitale Privatsphäre, S. 349.

206 *Weichert*, DANA 2/2013, 53 (55); vgl. *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 192; a. A. *v. Lewinski*, in: Auernhammer, § 1 BDSG, Rn. 19.

207 Vgl. zur privaten Videoüberwachung EuGH, Urteil v. 11.12.2014 – C-212/13, BeckRS 2014, 82595, Rn. 33.

208 Unter dem Begriff der Datenverarbeitungsanlage ist jede Vorrichtung zu verstehen, die in einem automatisierten Prozess Daten verwendet, insbesondere jegliche Art von Computern.

209 *Dammann*, in: Simitis, § 1 BDSG, Rn. 140; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 1 BDSG, Rn. 10.

210 Siehe *Gola/Schomerus*, § 3 BDSG, Rn 15, 15a; *Schwenke*, K&R 2013, 685 (689).

211 *Schwenke*, K&R 2013, 685 (689).

6.1.2 Anwendbarkeit des Telemediengesetzes

Vor einer möglichen Anwendung des BDSG ist zu untersuchen, ob bereichsspezifisches Datenschutzrecht gem. § 1 Abs. 3 S. 1 BDSG vorrangig ist. Im Rahmen von Google Glass kommt das Telemedienrecht mit bereichsspezifischen Vorschriften im Telemediengesetz (TMG) in Betracht. Es ist zu prüfen, inwiefern die datenschutzrechtlichen Regelungen des TMG auf Google Glass anwendbar sind und dem BDSG vorgehen.

Telemedien oder Telemediendienste werden negativ definiert und sind gem. § 1 Abs. 1. S. 1 TMG alle elektronischen Informations- und Kommunikationsdienste (I&K-Dienste), soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 Telekommunikationsgesetz (TKG) sind, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages darstellen. Bei Telemedien muss es sich demnach um elektronische I&K-Dienste handeln. Dies bedeutet, dass die Dienstleistung selbst elektronisch erbracht werden muss. Da Telemediendienste nicht zum Bereich der Übertragung, also Telekommunikation gehören, ist es entscheidend, ob die für den Dienst erforderlichen Inhalte elektronisch bereitgestellt werden.[212]

Laut des Gesetzgebers erstrecken sich Telemediendienste auf einen weiten Bereich von wirtschaftlichen Tätigkeiten, die u. a. über Abruf- oder Verteildienste elektronisch in Form von Bild-, Text- oder Toninhalten zur Verfügung gestellt werden. Darunter fallen die meisten Online-Dienste wie Informationsseiten, Blogs und Portale[213] sowie Suchmaschinen, soziale Netzwerke und Online-Rollenspiele.[214] Google Glass ermöglicht es durch die ständige Anbindung an das Internet Informationen in Bild-, Text- oder Toninhalten abzurufen und diese In-

[212] *Holznagel/Ricke*, in: Spindler/Schuster, § 1 TMG, Rn. 4.
[213] BT-Drs. 16/3078, S. 13 f.; weitere Beispiele bei *Müller-Broich*, § 1 TMG, Rn. 6.
[214] *Jotzo*, MMR 2009, 232 (234) m. w. N.

formationen aufzubereiten und jederzeit anzuschauen. Demzufolge ist Google Glass ein Telemedium i. S. v. § 1 Abs. 1 S. 1 TMG und Google als Diensteanbieter gleichwohl Adressat der Vorschriften des TMG. Der Glass-Träger hingegen fällt nicht in den Adressatenkreis dieses Gesetzes, da er das Kriterium des Diensteanbieters nicht erfüllt, sondern lediglich das Telemedium Google Glass in Anspruch nimmt.

Gem. § 1 Abs. 3 S. 1 BDSG gehen die in den § 11 ff. TMG enthaltenen speziellen Datenschutzregelungen den Vorschriften des BDSG vor.[215] Im Rahmen dieser Arbeit hat das TMG für die zu behandelnden personenbezogenen Daten jedoch keine Bedeutung. Die Datenschutzvorschriften der §§ 11 ff. TMG und insbesondere die §§ 14 und 15 TMG regeln nämlich nur die Bestands-, Nutzungs- und Abrechnungsdaten, die hinsichtlich der Bereitstellung und Nutzung eines Telemediendienstes anfallen.[216] Darunter fallen solche Daten, die Google von dem Nutzer benötigt, um ihm die Dienste und Anwendungen[217] von Google Glass zur Verfügung zu stellen.[218] In diesem Fall wären dies die personenbezogenen Daten des Glass-Trägers, die für die Durchführung des Vertragsverhältnisses notwendig sind z. B. Name, Anschrift, E-Mail-Adresse, Alter oder Bankdaten sowie diejenigen personenbezogenen Daten wie die IP-Adresse, die während der Nutzung eines Telemediums entstehen und die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen.[219] Im Fokus dieser Arbeit stehen jedoch vielmehr die Inhaltsdaten. Darunter sind alle weiteren personenbezogenen Daten zu verstehen, die der Glass-Träger und der Diensteanbieter zwar online austauschen, die aber gerade nicht die Inanspruchnahme des Telemediendienstes ermöglichen.[220] Zu diesen Inhaltsdaten gehören etwa die vom Glass-Träger aufgenommenen

---

215 *Roßnagel*, in: Roßnagel, Einf., Rn. 43.
216 *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 6.
217 Siehe Kap. 2.2.
218 Hier ist auf die Literatur des Cloud-Computing zu verweisen z. B. *Kroschwald*, Informationelle Selbstbestimmung in der Cloud.
219 *Müller-Broich*, § 14 TMG, Rn. 2; § 15 TMG, Rn. 1; *Spindler/Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 2; *Dix*, in: Roßnagel, § 14 TMG, Rn. 22.
220 *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 27.

Inhalte, wie Fotos oder Videos. Diese Daten lassen sich nicht den Bestands- und Nutzungsdaten zuordnen, sodass die speziellen Datenschutzvorschriften des TMG darauf keine Anwendung finden. Für diese Inhaltsdaten findet grundsätzlich das BDSG Anwendung.[221] Somit bestimmt sich die Zulässigkeit des Umgangs von Google Glass erfassten Daten mangels lex specialis im TMG nach dem BDSG.

6.1.3 Verantwortliche Stelle

Die Vorschriften des BDSG richten sich, für die Frage der Zulässigkeit des jeweiligen Datenumgangs sowie der Verantwortlichkeit gegenüber Betroffenen, in erster Linie an die verantwortliche Stelle. Einschlägige Norm hierfür ist § 3 Abs. 7 BDSG, wonach verantwortliche Stelle jede Person oder Stelle ist, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. § 3 Abs. 7 BDSG setzt die Vorgabe des Art. 2 lit. d S. 1 DSRL in nationales Recht um, sodass für eine Bestimmung der Verantwortlichkeit im Einzelfall auf die Definition der verantwortlichen Stelle aus der DSRL zurückgegriffen werden kann.[222] Danach ist ein „für die Verarbeitung Verantwortlicher" die Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eine solche Entscheidungsmacht kann sich aus gesetzlicher oder impliziter Zuständigkeit ergeben.[223] Eine Stelle ist dann verantwortliche Stelle, wenn sie in der Lage ist, auf die Mittel und Zwecke der Verarbeitung Einfluss zu nehmen. Die Entscheidung über das Mittel der Datenverarbeitung umfasst technische und organisatorische Aspekte – also das „Wie" der Datenverarbeitung.[224] Während die Entscheidung über die

---

221 *Enzmann/Roßnagel*, CR 2002, 142; *Spindler/Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 3; *Dix*, in: Roßnagel, § 14 TMG, Rn. 17; *Bäumler*, DuD 1999, 259; BT-Drs. 14/5555, 65; *Zscherpe*, in: Taeger/Gabel, § 14 TMG, Rn. 19; *Jandt/Roßnagel*, MMR 2011, 637 (639); *Ernst*, NJOZ 2010, 1917 (1918); *Spindler/Nink*, in: Spindler/Schuster, § 11 TMG, Rn. 6.

222 *Plath/Schreiber*, in: Plath, § 3 BDSG, Rn. 66.

223 Art 29 Datenschutzgruppe, WP 169, S. 12.

224 Art. 29 Datenschutzgruppe, WP 169, S. 17; z. B. welche Hard-und Software eingesetzt wird, sowie Art der Daten, Speicherdauer und Zugriffsmöglichkeiten.

Mittel lediglich ein Indiz für die Verantwortung ist und die Einordnung von der Reichweite der Entscheidungsbefugnis über die Mittel abhängt, ist die Entscheidung über den Zweck – also das „Warum“[225] der Datenverarbeitung – letztlich die Schwelle für die Begründung datenschutzrechtlicher Verantwortlichkeit.[226]

In einer vernetzten Welt allgegenwärtiger Datenverarbeitung, die in vielfältigster Form und mit unterschiedlichsten Beteiligten erfolgt, gestaltet sich die Beantwortung der Frage, wer verantwortliche Stelle ist, durchaus diffizil.[227] Infolgedessen stellt sich diese Problematik bei der Nutzung von Google Glass. Daher ist in Bezug auf den pluralistischen Ansatz, den die DSRL mit der Formulierung „allein oder gemeinsam“ gibt,[228] zu untersuchen, ob in diesem Fall eine kollektive Verantwortung des Glass-Trägers, Google und ggf. dritten Diensteanbietern vorliegen könnte. Dies hätte zur Folge, dass die Beteiligten arbeitsteilig für bestimmte Daten und bestimmte Phasen des Datenumgangs verantwortlich sind.[229] Um eine kollektive Verantwortlichkeit feststellen zu können, werden im Folgenden die Verantwortlichkeiten nach einzelnen Vorgängen und Gegebenheiten differenziert.

6.1.3.1 Glass-Träger

Zunächst ist zu prüfen, inwiefern der Glass-Träger über die Mittel und Zwecke des Umgangs mit personenbezogenen Daten entscheidet und verantwortliche Stelle i. S. v. § 3 Abs. 7 BDSG ist.

Google bietet durch Google Glass den Nutzern einen technischen organisatorischen Rahmen und liefert durch entsprechende Glassware

---

225 Art. 29 Datenschutzgruppe, WP 169, S. 16; *Jandt/Roßnagel*, ZD 2011, 160; *Kroschwald*, informationelle Selbstbestimmung in der Cloud, S. 125.

226 Art. 29 Datenschutzgruppe, WP 169, S. 18; *Jandt/Roßnagel,* ZD 2011, 160.

227 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 63, Art. 29-Datenschutzgruppe, WP 169, S. 21; so auch für soziale Netzwerke siehe *Jandt/Roßnagel,* ZD 2011, 160, zum Cloud-Computing *Kroschwald*, Informationelle Selbstbestimmung in der Cloud.

228 *Jandt/Roßnagel,* ZD 2011, 160 (161); *Schenk/Niemann/Reinmann/Roßnagel*, Digitale Privatsphäre, S. 347.

229 *Jandt/Roßnagel*, ZD 2011, 160 (161).

vielfältige individuelle Handlungsmöglichkeiten über welche die Nutzer frei entscheiden können. Die Entscheidungsmacht von Google liegt lediglich bei den technischen und organisatorischen Mitteln und Formen der Datenverarbeitung.[230] Letztlich entscheidet der Glass-Träger alleine über die Zwecke des Datenumgangs bzw. was er mit der Datenbrille fotografiert und filmt. Demzufolge gibt Google zwar das Mittel der Datenverarbeitung vor, doch der Glass-Träger bestimmt alleine, welche konkreten Daten, zu welchen Zwecken und Umständen verarbeitet werden.[231] Aus diesen Gründen ist zu analysieren für welche Daten und in welchen Phasen des Datenumgangs dem Glass-Träger die datenschutzrechtliche Verantwortlichkeit gem. § 3 Abs. 7 BDSG zukommen könnte.

Der Glass-Träger könnte für die Erhebung personenbezogener Daten gem. § 3 Abs. 3 BDSG verantwortlich sein. Erheben ist das gezielte Beschaffen von Daten über Betroffene. Die Erhebung bedingt eine Aktivität der erhebenden Stelle, durch welche diese Kenntnis oder zumindest Verfügungsmacht erhält.[232] Ein solches Erheben ist u. a. die gezielte Kamera- und Tonaufnahme sowie die GPS-gestützte Lokalisierung von Dritten mittels Google Glass.[233] Weiter können auch Daten über Verhältnisse des Betroffenen wie sein Gewicht, Größe, Aussehen, Ort und Zeit des Aufenthaltes Ziel der Erhebung sein.[234] Auch ein solches Erheben ist durch spezifische Glassware, die Personen analysieren und vermessen kann, leicht zu verwirklichen. Die erhobenen Daten müssen stets einen Personenbezug und Bestimmbarkeit des Betroffenen gewährleisten. Dies ist durch Beobachten bzw. Kameraaufnahmen grundsätzlich gegeben.[235] Etwas anderes könnte sich bei reinen Tonaufnahmen ergeben, die ebenso wie anonyme Telefonbera-

230 Vgl. *Jandt/Roßnagel*, ZD 2011, 160 (161).
231 Ähnlich wie bei Social Networks *Jandt/Roßnagel*, ZD 2011, 160 (161).
232 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 3 BDSG, Rn. 30, 31; *Dammann*, in: Simitis, § 3 BDSG, Rn. 102, 104.; *Schild*, in: Roßnagel, Hdb DS, 4.2, Rn. 37; *Gola/Schomerus*, § 3 BDSG, Rn. 24.
233 *Schild*, in: Roßnagel, Hdb DS, 4.2, Rn. 35; *Dammann*, in: Simitis, § 3BDSG, Rn. 105.
234 *Dammann*, in: Simitis, § 3 BDSG, Rn. 105.
235 *Dammann*, in: Simitis, § 3 BDSG, Rn. 108, 109.

tung nicht unter das Erheben fallen.[236] Allerdings ermöglicht Google Glass durch seine vielfältigen Funktionen, entsprechende Zusatzinformationen zu der Tonaufnahme zu erheben. In diesem Fall könnte erneut ein Personenbezug gegeben sein. Folglich entscheidet der Glass-Träger selbst für welche Zwecke und Umstände er diese Daten erhebt und ist demnach verantwortlich für die Datenerhebung gem. § 3 Abs. 7 BDSG.

Weiter ist zu prüfen, inwiefern der Glass-Träger für das Verarbeiten der Daten verantwortlich i. S. v. § 3 Abs. 7 BDSG sein könnte. Nach § 3 Abs. 4 BDSG fällt unter den Begriff des Verarbeitens das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. In den aufgeführten Szenarien kommt überwiegend eine Verarbeitung in Form des Speicherns und Übermittelns in Betracht, sodass für diese Vorgänge die Verantwortlichkeit geprüft werden muss.[237] Grundsätzlich erfolgt vor einer Verarbeitung die Erhebung personenbezogener Daten, demnach können die oben beschriebenen Daten für die Bewertung herangezogen werden.

Das Speichern nach § 3 Abs. 4 Nr. 1 BDSG ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung. Wie in Kapitel 2.2 beschrieben besitzt Google Glass einen internen Speicher, der dem Nutzer ermöglicht erhobene Daten zu speichern. In diesem Fall bestimmt der Glass-Träger selbst, zu welchen Zwecken er die Daten auf der Datenbrille speichert. Für die Speicherung lässt sich somit eine datenschutzrechtliche Verantwortlichkeit i. S. v. § 3 Abs. 7 BDSG begründen.

Ein Übermitteln gem. § 3 Abs. 4 Nr. 3 BDSG ist das Bekanntgeben personenbezogener Daten an einen Dritten durch Datenweitergabe oder durch Einsicht bzw. Abruf bei entsprechender Bereithaltung.[238] Eine

---

236 *Dammann*, in: Simitis, § 3 BDSG, Rn. 110.

237 Auffangtatbestand dazu ist das Nutzen nach § 3 Abs. 5 BDSG, dies liegt z. B. bei einer Auswertung von Daten oder internen Abruf vor.

238 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 3 BDSG, Rn. 36.

Übermittlung setzt nicht voraus, dass die Empfänger konkret bekannt sind, also genügt die Bekanntgabe gegenüber der Öffentlichkeit oder einer bestimmten Personengruppe. Das Einstellen von Daten ins Internet zum Abruf, ist eine Veröffentlichung und damit eine Übermittlung mit der bzgl. des Empfängerkreises höchsten vorstellbaren Eingriffsintensität.[239] Google Glass ist ständig mit dem Internet verbunden und auch dafür konzipiert worden, Informationen im Internet zu veröffentlichen oder in sozialen Netzwerken zu teilen. Teilt der Glass-Träger seine erfassten personenbezogenen Daten im Internet oder einem sozialen Netzwerk, entscheidet dieser selbst über die Zwecke der vorliegenden Übermittlung.[240] Infolgedessen ist dem Glass-Träger in diesem Fall die Verantwortlichkeit gem. § 3 Abs. 7 BDSG zuzuschreiben.

Zusammenfassend ist der Glass-Träger für die Phasen der Erhebung, Speicherung und Übermittlung von personenbezogenen Daten nach § 3 Abs. 3 und 4 BDSG die verantwortliche Stelle, da er i. S. v. § 3 Abs. 7 BDSG über das „Warum" der Datenverarbeitung alleine entscheidet.

6.1.3.2 Google

Wie oben bereits ermittelt, stellt Google die technischen und organisatorischen Mittel im Rahmen der Funktionalität der Datenbrille für den Datenumgang zur Verfügung. Weiter ist zu prüfen, inwiefern Google auch über die Zwecke eines Datenumgangs entscheidet und sich demgemäß auch eine datenschutzrechtliche Verantwortlichkeit für das Unternehmen i. S. v. § 3 Abs. 7 BDSG begründen lassen könnte.

Alle vom Glass-Träger erfassten Daten werden automatisch auf den Google-Servern gespeichert, sodass dies unter die Verarbeitung personenbezogener Daten nach § 3 Abs. 4 Nr. 1 BDSG zu subsumieren ist.

---

[239] Zudem ist § 22 KUG heranzuziehen, vgl. *Gola*, NJW 2000, 3749 (3752); *Brühann*, DuD 2004, 201 (203 f.); *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 36; VG Wiesbaden, MMR 2009, 430.

[240] Vgl. Kap. 6.1.3.3.

Ein Auftragsverhältnis i. S. v. § 11 BDSG kann allerdings ausgeschlossen werden, da es an einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag[241] und somit an Weisungen, die Google vertraglich hinsichtlich Art und Gegenstand des Datenumgangs und technischer sowie organisatorischer Maßnahmen übernimmt, fehlt.[242] Die Datenbrille ist an die Google-Infrastruktur gebunden, d. h. die vom Nutzer erfassten Daten werden von Google auf unternehmenseigenen Servern gespeichert, um u. a. Glass-Anwendungen zur Verfügung zu stellen, die Dienste weiterzuentwickeln und es den Nutzern zu erleichtern, Kontakte mit anderen zu knüpfen.[243] Um die individuelle Nutzung der Datenbrille zu ermöglichen, entscheidet Google neben dem „Wie" ebenso über das „Warum" der Speicherung auf den unternehmenseigenen Servern. Aus diesem Grund kann Google für diese Phase des Datenumgangs als verantwortliche Stelle gem. § 3 Abs. 7 BDSG betrachtet werden.[244]

Fraglich ist, ob Google gleichzeitig für die Übermittlung der Daten i. S. v § 3 Abs. 4 Nr. 3 BDSG auf die Google-Server verantwortlich ist. Erst durch die Speicherung der Daten auf den unternehmenseigenen Servern ist es Google möglich, den Nutzern das volle Potenzial der Datenbrille zu liefern. Dafür bedarf es der Übermittlung der vom Nutzer erfassten Daten auf die Server. In diesem Fall legt Google ebenfalls im Voraus die technischen und organisatorischen Mittel fest und entscheidet über den Zweck der Übermittlung. Infolgedessen ist Google für das Übermitteln der vom Nutzer erfassten Daten auf die unternehmenseigenen Server verantwortlich gem. § 3 Abs. 7 BDSG.

Während Google für diese Übermittlung die Hauptverantwortlichkeit zugeschrieben wird, ist gleichwohl die Rolle des Glass-Trägers zu beachten. Diesem könnte allenfalls eine ergänzende Verantwortlichkeit

---

241 *Plath*, in: Plath, § 11 BDSG, Rn. 21; *Gola/Schomerus*, § 11 BDSG, Rn. 6; *Petri*, in: Simitis, § 11 BDSG, Rn. 1.

242 *Rammos/Böhm*, in: Gierschmann/Saeugling, § 11 BDSG, Rn. 33; *Gola/Schomerus*, § 11 BDSG, Rn. 24; *Petri*, in: Simitis, § 11 BDSG, Rn. 85.

243 Kap. 2.2.

244 So auch *Weichert*, DANA 2/2013, 53 (55).

zu kommen. Der Träger selbst entscheidet zwar nicht über die Mittel der Datenverarbeitung, jedoch könnte dieser mittelbar den Zweck der Übermittlung beeinflussen. Dies ergibt sich durch den Kaufvertrag[245] über die Google Glass, indem dieser davon Kenntnis erlangt, dass die von ihm erfassten Daten automatisch an Google-Server übermittelt, gespeichert und synchronisiert werden. Aus diesem Grund ist davon auszugehen, dass dem Nutzer bewusst ist, dass seine erhobenen Daten zwangsläufig automatisch an Google übermittelt werden. Somit könnte dem Glass-Träger zumindest eine ergänzende Verantwortlichkeit für das Übermitteln gem. § 3 Abs. 7 BDSG treffen.

Im Rahmen der datenschutzrechtlichen Verantwortlichkeit von Google bleibt allerdings offen, ob und zu welchen Zwecken die auf den Servern gespeicherten Daten von Google weiterverarbeitet werden, sodass lediglich auf die mangelnde Vorhersehbarkeit künftiger Nutzung in Kapitel 4.3 zu verweisen ist.

6.1.3.3 Andere Diensteanbieter

Aufgrund der Leichtigkeit die von Google Glass aufgenommenen Fotos oder Videos im Internet und sozialen Netzwerken mit anderen teilen zu können, ist zu prüfen, inwiefern andere Diensteanbieter, die entsprechende Glassware wie z. B. Facebook zur Verfügung stellen, aus datenschutzrechtlicher Sicht verantwortlich sein könnten.[246] Maßgeblich hierfür ist, wer über die Mittel und den Zweck des Datenumgangs entscheidet. Soweit der Plattformanbieter den Zweck verfolgt, Daten seiner Nutzer für personalisierte Werbung auszuwerten und diese Werbemöglichkeit zu verkaufen,[247] besteht ein klassisches datenschutzrechtliches Verhältnis zwischen dem Anbieter als verantwortliche Stelle und dem Nutzer als Betroffener.[248] Der Anbieter entscheidet demnach allein über die erfassten Daten, den Zweck der Datenverar-

[245] Term of Use - Google Glass, Internetquelle
[246] Siehe auch *Bartelt*, Datenschutz in sozialen Netzwerken, S. 41.
[247] *Bartelt*, Datenschutz in sozialen Netzwerken, S. 15 f.
[248] *Jandt/Roßnagel*, ZD 2011, 160 (161).

beitung und die Art und Weise wie sie erfolgt.[249] Dafür stellt der Anbieter den Nutzern eine Plattform zur Verfügung, auf der sie „Communities" bilden und weitere personenbezogene Daten erzeugen können.[250] Dort entscheidet der Daten eingebende Nutzer, welche personenbezogenen Daten Dritter er erhebt und auswählt, welchen Zweck er mit ihnen verfolgt, inwiefern er sie verbreitet und wie lange sie verfügbar sind.[251] Die Entscheidungsmacht des Anbieters ist lediglich auf das Angebot der technischen und organisatorischen Mittel und Formen der Datenverarbeitung beschränkt.[252] Demgemäß sind die Anbieter sozialer Netzwerkdienste für die Daten und Phasen des Umgangs verantwortlich, soweit sie sowohl über die Zwecke als auch die Mittel des Umgangs mit personenbezogenen Daten von Nutzern und Dritten entscheiden. Der Glass-Träger ist verantwortlich, sobald dieser personenbezogene Daten Dritter über das soziale Netzwerk erhebt, veröffentlicht oder auf sonstige Art und Weise verarbeitet.[253] In diesem Fall kommt zusätzlich die in Kap. 6.1.3.2 erläuterte Verantwortlichkeit von Google hinzu, da alle vom Glass-Träger erfassten Daten auf den Google-Server übermittelt und gespeichert werden, bevor der Nutzer sie in sozialen Netzwerken teilen kann. Es ist daher in solchen Konstellationen stets zwischen den einzelnen Phasen und Zwecken des Datenumgangs zu differenzieren, um eine eindeutige Verantwortlichkeit für die jeweilige Phase des Datenumgangs feststellen zu können.

6.1.3.4 Zwischenfazit

Anhand der soeben geprüften datenschutzrechtlichen Verantwortlichkeiten der i. R. v. Google Glass Beteiligten, konnte die zu Beginn des Abschnitts aufgeführte These einer kollektiven Verantwortlichkeit belegt werden. Demzufolge gibt es bei der Nutzung von Google Glass

---

249 *Jandt/Roßnagel*, ZD 2011, 160 (161); *Erd*, NVwZ 2011, 19; *Kroschwald*, ZD 2013, 388 (389).

250 *Jandt/Roßnagel*, ZD 2011, 160 (161).

251 *Schwenk/Niemann/Reinmann/Roßnagel*, Digitale Privatsphäre, S. 347 f; *Jandt/Roßnagel*, ZD 2011 160 (161).

252 *Jandt/Roßnagel*, ZD 2011, 160 (161).

253 Art. 29-Datenschutzgruppe, WP 169, S. 26.

mehrere verantwortliche Stellen für bestimmte Phasen des Datenumgangs. Eine kumulative Verantwortlichkeit dieser Stellen scheidet jedoch aus, da die Beteiligten nicht für alle Daten und Phasen des Datenumgangs verantwortlich sind.[254] Die genannten Stellen kontrollieren den Datenumgang nicht gemeinschaftlich, sondern vielmehr getrennt und bezogen auf unterschiedliche Phasen der Datenverarbeitung.[255] Festzuhalten ist, dass sich die Verantwortungsbereiche von Glass-Trägern, Google und Drittanbietern nicht überschneiden, sondern kollektiv nebeneinander stehen.[256] Der Glass-Träger ist datenschutzrechtlich verantwortlich soweit dieser personenbezogene Daten Dritter erhebt und verarbeitet. Hingegen ist Google für die dargestellten Phasen des Datenumgangs verantwortlich, sofern das Unternehmen über die Mittel und Zwecke der Datenverarbeitung mit personenbezogenen Daten von Nutzern und Dritten entscheidet. Des Weiteren ist u. a. die Verantwortlichkeit von Anbietern sozialer Netzwerke zu berücksichtigen. Demzufolge gibt es bei der Nutzung von Google Glass nicht nur eine datenverarbeitende Stelle, die die Kriterien des § 3 Abs. 7 BDSG erfüllt. Im Gegenteil, in diesem Fall ist von einer kollektiven Verantwortlichkeit aller Beteiligten auszugehen, die stets im Einzelfall zu beurteilen ist. Aus diesem Grund ist die folgende datenschutzrechtliche Zulässigkeitsprüfung getrennt für den Glass-Träger und Google als verantwortliche Stelle i. S. v. § 3 Abs. 7 BDSG durchzuführen.

6.2 Datenschutzrechtliche Zulässigkeit

Soeben wurden die Anwendbarkeit des BDSG und die verantwortliche Stelle, für die jeweiligen Phasen des Datenumgangs, als dessen Normadressat bestimmt. Nachfolgend sind die Voraussetzungen für die Zulässigkeit eines Datenumgangs im Rahmen von Google Glass zu untersuchen. Um die Sicherung des informationellen Selbstbe-

254 *Jandt/Roßnagel*, ZD 2011, 160 (161), *Kroschwald* ZD 2013, 388 (389), *Schwenk/Niemann/Reinmann/Roßnagel*, Digitale Privatsphäre, S. 348.
255 So auch *Kroschwald*, ZD 2013, 388 (389).
256 Vgl. *Jandt/Roßnagel* ZD 2011, 160 (161).

stimmungsrechts zu schützen,[257] ist gem. § 4 Abs. 1 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Daher ist grundsätzlich jeder Umgang mit personenbezogenen Daten einzeln und in Bezug auf die konkrete datenverarbeitende Stelle zu überprüfen. Als gesetzlicher Erlaubnistatbestand kommt jede Rechtsvorschrift in Betracht, die den Umgang mit personenbezogenen Daten ausdrücklich zulässt oder anordnet.[258] Alle materiellen Rechtsnormen mit unmittelbarer Außenwirkung, insbesondere Gesetze und Rechtsverordnungen, sind als „Rechtsvorschrift" zu verstehen.[259] Auch Satzungen mit Rechtsnormqualität sowie normative Teile von Tarifverträgen und Betriebsvereinbarungen sind Rechtsvorschriften i. S. d. § 4 Abs. 1 BDSG.[260]

Im Folgenden sind die möglichen einschlägigen Erlaubnistatbestände des BDSG für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen der Nutzung von Google Glass zu prüfen.

6.2.1 Datenumgang durch die Google Glass-Träger

Aufgrund der kollektiven Verantwortlichkeit[261] ist in den folgenden Ausführungen zunächst zu untersuchen, inwiefern sich der Datenumgang der Glass-Träger durch Vorschriften des BDSG rechtfertigen lassen könnte. Die datenschutzrechtliche Bewertung orientiert sich dazu an den in Kapitel 3 beschriebenen Szenarien.

6.2.1.1 Rechtfertigung durch § 6b BDSG

Werden mit Google Glass in den Szenarien aus Kapitel 3 Videoaufnahmen von anderen Personen angefertigt, könnte sich zunächst de-

257 *Scholz/Sokol*, in: Simitis, § 4 BDSG, Rn. 2.
258 *Taeger*, in: Taeger/Gabel, § 4 BDSG, Rn. 21.
259 *Scholz/Sokol*, in: Simitis, § 4 BDSG, Rn. 9.
260 BAGE 52, 88 (102 ff.); *Taeger*, in: Taeger/Gabel, § 4 BDSG, Rn. 35; *Gola/Schomerus*, § 4 BDSG, Rn. 7; *Scholz/Sokol*, in: Simitis, § 4 BDSG, Rn. 10, 11.
261 Kap. 6.1.3.

ren Zulässigkeit nach § 6b BDSG richten. Danach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen für nicht-öffentliche Stellen ausschließlich gem. § 6b Abs. 1 Nr. 2 und 3 BDSG zur Wahrung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke zulässig. In diesen Fällen ist die Videoüberwachung lediglich erlaubt, wenn sie nach § 6b Abs. 3 BDSG zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Anwendung dieser Vorschrift setzt die generelle Anwendbarkeit des BDSG voraus. Sie kommt deshalb auch für die in § 1 Abs. 2 Nr. 3 BDSG genannten nicht-öffentlichen Stellen zur Anwendung, wenn die Überwachung in öffentlich zugänglichen Räumen erfolgt.[262] Bei der Videoaufnahme müsste es sich um eine Beobachtung[263] i. S. d. § 6b Abs. 1 BDSG handeln. Darunter ist die Sichtbarmachung von Geschehnissen und Personen mit Hilfe dazu geeigneter technischer Einrichtung zu verstehen.[264] Google Glass lässt sich unter den Begriff der optisch-elektronischen Einrichtung subsumieren, da sie sich aufgrund ihrer Videoaufnahmefunktion für Beobachtungen grundsätzlich eignet.[265] Der Vorgang der Beobachtung setzt eine gewisse zeitliche Dauer voraus,[266] sodass die Regelung auf einmalige Bilderfassungen i. d. R. nicht anwendbar ist.[267] Demgegenüber kann der bereits zeitweise Betrieb einer Kamera das Vorliegen einer Beobachtung begründen.[268] Google Glass ist hauptsächlich dazu gedacht

---

[262] *v. Zezschwitz*, in: Roßnagel, Hdb DS, 9.3, Rn. 14; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 6b BDSG, Rn. 2; *Becker*, in: Plath, § 6b BDSG, Rn. 3.

[263] Beobachten ist ein besonderer Fall des Erhebens, siehe Kapitel 6.1.3.1.

[264] *Scholz*, in: Simitis, § 6b BDSG, Rn. 63; *Zscherpe*, in: Taeger/Gabel, § 6b BDSG, Rn. 17; *Gola/Schomerus*, § 6b BDSG, Rn. 10.

[265] *Scholz*, in: Simitis, § 6b BDSG, Rn. 36; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 6b BDSG, Rn. 16.

[266] *Gola/Schomerus*, § 6b BDSG, Rn. 12; *Scholz*, in: Simitis, § 6b BDSG, Rn. 64; *Zscherpe*, in: Taeger/Gabel, § 6b BDSG, Rn. 21.

[267] *Gola/Schomerus*, § 6b BDSG, Rn. 12.

[268] *Scholz*, in: Simitis, § 6b BDSG, Rn. 64; *Becker*, in: Plath, § 6b BDSG, Rn. 11; *Wiegand*, in: Gierschann/Saeugling, § 6b BDSG, Rn. 22; *Zscherpe*, in: Taeger/Gabel, § 6b BDSG, Rn. 21.

temporär lokal wechselnde Szenarien aufzunehmen.[269]. Insoweit ist im Einzelfall zu beurteilen, ob der geforderte zeitliche Moment gegeben ist. Gleichwohl setzt der Tatbestand der Beobachtung die Erhebung von personenbezogenen Daten voraus. Dafür reicht es aus, wenn öffentliche Räume in einer Art und Weise gefilmt werden, die es ermöglicht, bestimmte Personen zu identifizieren.[270] Die Beobachtung darf nicht gezielt auf Personen gerichtet sein,[271] sondern öffentlich zugängliche Räume erfassen. Darunter sind Bereiche innerhalb oder außerhalb von Gebäuden zu verstehen, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können und ihrem Zweck nach auch dazu bestimmt sind.[272] Es bleibt allerdings fraglich, ob der Glass-Träger tatsächlich nur öffentlich zugängliche Räume beobachtet. Naheliegend ist, dass der Mensch grundsätzlich eher Personen, als den gesamten Raum beobachtet.[273]

Zudem reicht es für die Zulässigkeit der Videoüberwachung mit Google Glass nicht aus, dass der Glass-Träger sein Hausrecht nach § 6b Abs. 1 Nr. 2 BDSG oder berechtigte Interessen für konkret festgelegte Zwecke gem. § 6b Abs. 1 Nr. 3 BDSG wahren möchte. Vielmehr müsste die Überwachung durch Google Glass für die Erreichung des Zwecks erforderlich sein. Dies wäre der Fall, soweit das Ziel mit Google Glass erreicht wird und es dafür kein anderes, gleich wirksames, aber mit Blick auf die informationelle Selbstbestimmung der betroffenen Personen weniger einschneidendes Mittel gibt.[274] Hinsichtlich des Einsatzes von Google Glass zur Überwachung bestehen Zweifel an der Erforderlichkeit. Fraglich ist bereits, ob sich Google Glass

---

269 *Solmecke/Kocatepe*, ZD 2014, 22 (25).

270 Eine Identifizierbarkeit liegt üblicherweise dann vor, wenn die Gesichtszüge erkennbar sind; *Wiegand*, in: Gierschmann/Saeugling, § 6b BDSG, Rn. 23; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 6b BDSG, Rn. 14; *Scholz*, in: Simitis, § 6b BDSG, Rn. 66.

271 *Scholz*, in: Simitis, § 6b BDSG, Rn. 67.

272 *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 6b BDSG, Rn. 19 ff.; *Scholz*, in: Simitis, § 6b BDSG, Rn. 42.

273 *Schwenke*, K&R 2013, 685 (690).

274 *Scholz*, in: Simitis, § 6b BDSG, Rn. 86; *Gola/Schomerus*, § 6b BDSG, Rn. 18a; *Zscherpe*, in: Taeger/Gabel, § 6b BDSG, Rn. 45.

dafür eignet, den angestrebten Überwachungszweck zu erreichen.[275] Um den Überwachungszweck bzw. eine angemessene Beobachtung durchführen zu können, müsste sich der Glass-Träger ständig in dem zu überwachenden Raum aufhalten. Ein weiterer Nachteil wäre die begrenzte Akkulaufzeit der Datenbrille, sodass grundsätzlich herkömmliche Videoüberwachungskameras eine effizientere und zugleich mildere Lösung darstellen. Hinzu kommt, dass die Beobachtung durch einen Glass-Träger genauso unberechenbar durch den Raum erfolgt wie sich der Mensch in diesem bewegt. Es ist nicht möglich einer Beobachtung zu entkommen bzw. sich von dieser abzuwenden, wie es bei sichtbaren Kameras der Fall ist.[276] Besonders durch diese Unberechenbarkeit ist es problematisch eine solche Überwachung ausreichend gem. § 6b Abs. 2 BDSG kenntlich zu machen,[277] um die geforderte Transparenz für den Betroffenen zu geben.[278] Der Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a BDSG wird ebenfalls verletzt, da durch die Beobachtung mittels Google Glass mehr personenbezogene Daten erfasst werden könnten, als es für die Videoüberwachung eines öffentlichen Raums erforderlich ist. Außerdem darf nicht ungeachtet bleiben, dass die Videoaufnahmen automatisch auf den Google-Servern gespeichert werden, sodass ein verstärkter Eingriff in die informationelle Selbstbestimmung vorliegen würde. Aus den genannten Gründen wird eine fest installierte Kamera immer ein gleich geeignetes und milderes Mittel für Überwachungszwecke darstellen. Unabhängig davon, ob im Einzelfall § 6b BDSG die einschlägige Norm für Videoaufnahmen mittels Google Glass ist, wären sie in jedem Fall als unzulässig zu bewerten.[279]

---

275 *Zscherpe*, in: Taeger/Gabel, § 6b BDSG, Rn. 45; *Scholz*, in: Simitis, § 6b BDSG, Rn. 87.
276 *Schwenke*, K&R 2013, 685 (690).
277 *Weichert*, DANA 2/2013, 53 (55); *Schwenke*, K&R 2013, 685 (690).
278 *Gola/Schomerus*, § 6b BDSG, Rn. 23; *Zscherpe*, in: Taeger/Gabel, § 6b BDSG, Rn. 62; *Scholz*, in: Simitis, § 6b BDSG, Rn. 102.
279 *Schwenke*, K&R 2013, 685 (690); *Solmecke/Kocatepe*, ZD 2014, 22 (25); *Weichert*, DANA 2/2013, 53 (55).

6.2.1.2 Rechtfertigung durch § 28 BDSG

Es ist zu prüfen, ob sich die Nutzung von Google Glass durch die Vorschrift des § 28 BDSG rechtfertigen lassen könnte. § 28 BDSG findet Anwendung, soweit die in § 27 Abs. 1 BDSG formulierten Bedingungen erfüllt sind. Danach müssen personenbezogene Daten durch nicht-öffentliche Stellen unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden. Zudem betont § 27 Abs. 1 S. 2 BDSG, dass die Anwendung ausgeschlossen ist, soweit der Datenumgang ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In weiten Teilen wiederholt § 27 Abs. 1 BDSG die Regelungen des § 1 Abs. 2 BDSG, sodass unter Berücksichtigung der Ausführungen in Kapitel 6.1 die Bedingungen des § 27 Abs. 1 BDSG erfüllt sind und sich die Zulässigkeit von Google Glass durch § 28 BDSG ergeben könnte.

Als zentrale Erlaubnisnorm für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für nicht-öffentliche Stellen regelt § 28 BDSG den Datenumgang für eigene Geschäftszwecke.[280] Der Begriff der „eigenen Geschäftszwecke" ist inhaltsgleich mit dem der „eigenen Zwecke".[281] Darunter fallen Datenverarbeitungen, die als Hilfsmittel zur Erfüllung bestimmter anderer, eigener Zwecke der Daten verarbeitenden Stellen erfolgen.[282] Da es sich bei der Nutzung von Google Glass nicht um geschäftsmäßige i. S. v. § 29 BDSG,[283] sondern „eigene Zwecke" des Glass-Trägers handelt, ist § 28 BDSG die einschlägige Norm.

---

280 *Simitis*, in: Simitis, § 28 BDSG, Rn. 1; *Gierschmann*, in: Gierschmann/Saeugling, § 28 BDSG, Rn. 1; *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 89.

281 *Simitis*, in: Simitis, § 28 BDSG, Rn. 23, *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 30; *Gola/Schomerus*, § 28 BDSG, Rn. 4.

282 *Gola/Schomerus*, § 28 BDSG, Rn. 4; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 10; *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 14.

283 Zu Einzelheiten des § 29 BDSG *Gola/Schomerus*, § 29 BDSG; *Ehmann*, in: Simitis, § 29 BDSG.

§ 28 Abs. 1 BDSG enthält drei Zulässigkeitsvarianten, die grundsätzlich unabhängig voneinander die Zulässigkeit des Erhebens, Speicherns, Veränderns, Übermittelns und Nutzens von personenbezogenen Daten auch ohne Einwilligung des Betroffenen begründen können.[284] Dies gilt es für die Nutzung von Google Glass im Rahmen der beschriebenen Szenarien zu überprüfen.

6.2.1.2.1 Das rechtsgeschäftliche oder rechtsgeschäftsähnliche Schuldverhältnis

Zunächst ist zu prüfen, ob sich die Zulässigkeit des Datenumgangs durch den Glass-Träger in den vorher beschriebenen Szenarien durch § 28 Abs. 1 S. 1 Nr. 1 BDSG ergeben könnte. Danach ist der Datenumgang zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Vom Tatbestand des rechtsgeschäftlichen Schuldverhältnisses sind alle Arten von kausalen oder abstrakten Verträgen wie etwa Kauf-, Leih-, Werk-, Mietverträge erfasst.[285] Ein rechtsgeschäftsähnliches Schuldverhältnis könnte z. B. während der konkreten Anbahnung eines Schuldverhältnisses entstehen.[286]

Im Hinblick auf die vorgestellten Szenarien besteht kein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis zwischen dem Glass-Träger und den Betroffenen. Lediglich im Szenario 3.4 könnte ein rechtsgeschäftliches Schuldverhältnis in Form des Arbeitsvertrages zu sehen sein. Dazu müsste Google Glass für die Begründung, Durchführung oder Beendigung des Arbeitsvertrages erforder-

---

284 *Gola/Schomerus*, § 28 BDSG, Rn. 8; die drei Tatbestandsvarianten stehen zwar nach dem Wortlaut ohne Rangfolge nebeneinander, dennoch treten die Zulässigkeitstatbestände nach Nr. 2 und Nr. 3 hinsichtlich ihrer Anwendung hinter den der Nr. 1 zurück.

285 *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 19 m. w. N.; *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 39 ff.; *Gola/Schomerus*, § 28 BDSG, Rn. 12; *Simitis*, in: Simitis, § 28 BDSG, Rn. 56 ff.

286 *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 23; *Simitis*, in: Simitis, § 28 BDSG, Rn. 88; *Gola/Schomerus*, § 28 BDSG, Rn. 13.

lich sein und der Arbeitnehmer unter den Betroffenen subsumiert werden können. Allerdings kommt für den Bereich des Arbeitsverhältnisses die spezifische Regelung des § 32 BDSG in Betracht. Diese Norm gilt für alle Beschäftigungsverhältnisse und verdrängt die allgemeine Regelung des § 28 Abs. 1 S. 1 Nr. 1 BDSG.[287] Es sei insofern auf die Ausführungen dort verwiesen.[288] Demnach lässt sich die der Datenumgang durch den Glass-Träger nicht durch § 28 Abs. 1 S. 1 Nr. 1 BDSG rechtfertigen.

6.2.1.2.2 Wahrnehmung berechtigter Interessen

Der Datenumgang im Rahmen der Nutzung von Google Glass könnte nach § 28 Abs. 1 S. 1 Nr. 2 BDSG zulässig sein. Danach ist ein Datenumgang zur Wahrung berechtigter Interessen erlaubt, wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen der Verarbeitung oder Nutzung entgegensteht. Für den Fall, dass kein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis besteht, stellt § 28 Abs. 1 S. 1 Nr. 2 BDSG keinen Auffangtatbestand zu § 28 Abs. 1 S. 1 Nr. 1 BDSG dar.[289]

Berechtigte Interessen betreffen darüber hinaus grundsätzlich nur eigene Belange der verantwortlichen Stelle.[290] Unter den Begriff berechtigtes Interesse fällt jedes rechtliche, wirtschaftliche oder ideelle Interesse, das von der Rechtsordnung nicht missbilligt wird.[291] Ein solches Interesse kann daher jedes von der Rechtsordnung tolerierte Interesse sein.[292] Gleichwohl um welche Interessen es im Einzelnen geht, müssen diese immer mit der konkret beabsichtigten Verwendung zusam-

---

287 *Plath*, in: Plath, § 28 BDSG, Rn. 39; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 24; *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 30; *Zöll*, in: Taeger/Gabel, § 32 BDSG, Rn. 6.

288 Kap. 6.2.1.3.

289 *Simitis*, in: Simitis, § 28 BDSG, Rn. 99; anders *Plath*, in: Plath, § 28 BDSG, Rn. 46.

290 *Simitis*, in: Simitis, § 28 BDSG, Rn. 105; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 48; *Plath*, in: Plath, § 28 BDSG, Rn. 48.

291 Vgl. VGH Mannheim, NJW 1984, 1912; *Gola/Schomerus*, § 28 BDSG, Rn. 24; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 48; *Simitis*, in: Simitis, § 28 BDSG, Rn. 104; *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 231.

292 *Schaffland/Wiltfang*, § 28 BDSG, Rn. 85.

menhängen und sich auf Daten beziehen, die dabei verarbeitet werden sollen.[293] Aufgrund des Vorbehalts der Interessenabwägung, muss die Verwendung personenbezogener Daten zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich und nicht etwa aus der Sicht der verantwortlichen Stelle lediglich „geeignet" oder „zweckmäßig" sein.[294] Davon sind nur solche Verwendungen betroffen, zu denen es kein gleich geeignetes, weniger in das informationelle Selbstbestimmungsrecht einschneidendes Mittel zur Erreichung des Zwecks[295] bzw. keine objektiv zumutbare Alternative gibt.[296] Das bedeutet, dass § 28 Abs. 1 S. 1 Nr. 2 BDSG solange nicht zur Anwendung kommt, wie die verantwortliche Stelle ihr Informationsziel in anderer Weise erreichen kann.[297]

Sind berechtigte Interessen der verantwortlichen Stelle vorhanden und die Erforderlichkeit des Datenumgangs für die Wahrung dieser Interessen festgestellt worden, müssen anschließend die legitimen Interessen der verantwortlichen Stelle mit den schutzwürdigen Interessen des Betroffenen abgewogen werden. Im Hinblick auf § 1 Abs. 1 BDSG ist mit schutzwürdigen Interessen das Persönlichkeitsrecht des Betroffenen und insbesondere die informationelle Selbstbestimmung gemeint.[298] Die möglichen schutzwürdigen Interessen lassen sich anhand der jeweils spezifischen Verarbeitungssituation bzw. den jeweiligen Verarbeitungsbedingungen messen, gleichzeitig lassen sich daraus die Konsequenzen für den Betroffenen und das Maß der Beein-

---

293 *Simitis,* in: Simitis, § 28 BDSG, Rn. 102; *Gola/Schomerus*, § 28 BDSG, Rn. 25; *Schaffland/Wiltfang*, § 28 BDSG, Rn. 85.

294 *Simitis*, in: Simitis, § 28 BDSG, Rn. 125, 105, 108; *Gola/Schomerus*, § 28 BDSG, Rn. 25; *Gola/Klug*, Grundzüge des Datenschutzrechts, S. 91

295 Nach § 28 Abs. 1 S. 2 BDSG sollen zudem die Zwecke für den Datenumgang konkret festgelegt werden.

296 Vgl. auch BGH, NJW 1984, 1886 (1887); *Gola/Schomerus,* § 28 BDSG, Rn. 25; *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 235; *Simitis*, in: Simitis, § 28 BDSG, Rn. 108; *Gierschmann,* in: Gierschmann/Saeugling, § 28 BDSG, Rn. 42.

297 *Simitis*, in: Simitis, § 28 BDSG, Rn. 108; *Gola/Schomerus*, § 28 BDSG, Rn. 24; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 48; *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 59.

298 *Gola/Schomerus*, § 28 BDSG, Rn. 26; *Schaffland/Wiltfang*, § 28 BDSG, Rn. 86; *Taeger,* in: Taeger/Gabel, § 28 BDSG, Rn. 63; *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 236.

trächtigung bestimmen.[299] Weiter darf kein Grund zu der Annahme bestehen, dass die schutzwürdigen Interessen überwiegen. Die verantwortliche Stelle wird hiernach verpflichtet zu prüfen, ob sich ein Grund zu der Annahme bietet, dass der Datenumgang zu dem damit verfolgten Zweck schutzwürdige Belange des Betroffenen beeinträchtigt.[300] Liegt ein Grund zur Annahme einer solchen Beeinträchtigung vor, hat sie eine Interessenabwägung vorzunehmen, die sich am Verhältnismäßigkeitsgrundsatz auszurichten hat[301] und die Wertungen des BVerfG zum informationellen Selbstbestimmungsrecht berücksichtigen muss.[302] Bei der Abwägung sind Art, Inhalt und Aussagekraft der Daten mit den Aufgaben und Zwecken, denen der Datenumgang dient, zu beachten.[303]

6.2.1.2.2.1 Erforderlichkeit für die Wahrung berechtigter Interessen

Die in Kapitel 3 beschriebenen Szenarien könnten sich durch § 28 Abs. 1 S. 1 Nr. 2 BDSG rechtfertigen lassen, wenn ein berechtigtes und zugleich erforderliches Interesse des Glass-Trägers gegeben ist. An dieser Stelle ist Szenario 3.4 nicht zu prüfen, da es anhand des § 32 BDSG zu bewerten ist und nicht zusätzlich oder alternativ auf die Zulässigkeitsalternative des § 28 Abs. 1 S. 1 Nr. 2 BDSG zurückgegriffen werden kann.[304]

Google Glass ist, wie Szenario 3.1 zeigt, durchaus geeignet und zweckmäßig beim Sport unterstützend mitzuwirken. Fraglich ist, ob das Interesse Google Glass beim Sport zu nutzen erforderlich i. S. d. § 28 Abs. 1 S. 1 Nr. 2 BDSG ist. Unter Berücksichtigung der zahlrei-

---

299 *Simitis,* in: Simitis, § 28 BDSG, Rn. 127.

300 BGH, NJW 1984, 1889 (1890); ausreichend ist dabei zunächst eine summarische Prüfung, für die verantwortliche Stelle darf nicht schon von vornherein ein konkreter Umstand erkennbar sein, der auf ein schutzwürdiges, vom Persönlichkeitsrecht gedecktes Gegeninteresse schließen lässt.

301 BGH NJW 1984, 1889; BGH NJW 1984, 436; BGH, NJW 1986, 2505.

302 *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 239; BGH, NJW 1984, 1890.

303 BGH, NJW 1986, 2506; *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 139; *Simitis*, in: Simitis, § 28BDSG, Rn. 128.

304 *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 14; *Simitis*, in: Simitis, § 28 BDSG, Rn. 54.

chen Fitness-Gadgets wie Fitness-Armbänder, Pulsuhren, spezielle Smartphone-Apps und der Kamera Go Pro stellen diese im Vergleich zu Google Glass in jedem Fall gleich wirksame, aber im Blick auf die informationelle Selbstbestimmung der betroffenen Personen weniger einschneidende Mittel dar. Die Kamerafunktion sowie die Nutzung personenbezogener Daten Dritter ist während der Ausführung sportlicher Tätigkeiten und der Benutzung der Umkleidekabinen schlicht unnötig, sodass das Interesse Google Glass beim Sport zu nutzen nicht erforderlich scheint. Infolgedessen lässt sich die Nutzung von Google Glass im Szenario 3.1 nicht durch § 28 Abs. 1 S. 1 Nr. 2 BDSG rechtfertigen.

In Szenario 3.2 stellt Google Glass ein geeignetes und erfolgsversprechendes Hilfsmittel für das Flirtverhalten des Glass-Trägers dar. Dennoch ist dem Interesse, die Datenbrille als „Flirthilfe" zu nutzen, mit berechtigten Zweifeln hinsichtlich der Erforderlichkeit zu begegnen. Insbesondere durch die Möglichkeit der Gesichtserkennung und der Identifizierung unbemerkt fotografierter Menschen wird die Furcht vor dem gläsernen Menschen bestärkt.[305] Dementsprechend ist für die Partnersuche auf gleich gut geeignete und weniger in das informationelle Selbstbestimmungsrecht einschneidende Mittel zurückzugreifen. Partnerbörsen, Kontaktanzeigen und entsprechende Smartphone-Apps können als geeignete und mildere Alternative zum gleichen Erfolg führen.[306] Alldem vorzuziehen ist jedoch das eigene natürliche Flirtverhalten. Aufgrund fehlender Erforderlichkeit dieses Interesses ist die Nutzung von Google Glass im Rahmen des Szenario 3.2 gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG unzulässig.

Anders könnte das Interesse der Glass-Träger aus Szenario 3.3 zu bewerten sein. Bei Menschen mit medizinisch nachweisbaren physischen und/oder psychischen Defiziten äußert sich das berechtigte Interesse darin ein „normales" Leben führen zu können. Insbesondere für Men-

[305] Kap. 4; *Solmecke/Kocatepe*, ZD 2014, 22 (26); vgl. Art. 29-Datenschutzgruppe, WP 192.
[306] Z. B. Parship, Elitepartner etc.

schen mit Wahrnehmungs- und Informationsverarbeitungsstörungen bietet Google Glass eine enorme Erleichterung des Alltags. Mit der Datenbrille können diese Menschen die individuellen Barrieren sowie die Schwächen sozialer Interaktion und Kommunikation überwinden und eine kommunikative Basis schaffen, um wie alle anderen Menschen auch uneingeschränkt an der Gesellschaft teilnehmen zu können.[307] Fraglich ist, ob die Erhebung und Verarbeitung von personenbezogenen Daten betroffener Dritter durch den Glass-Träger für die Wahrung dieser berechtigten Interessen erforderlich ist. Hierzu müsste die Beseitigung vielfältiger Barrieren und die selbständige Teilnahme an der Gesellschaft bei vernünftiger Betrachtung ohne die Nutzung von Google Glass nicht möglich sein oder es zumindest nach den Gesamtumständen keine sinnvolle oder zumutbare Alternative geben.

Es gibt bereits viele Hilfsmittel für körperlich oder geistig beeinträchtigte Menschen, um ihnen das alltägliche Leben zu erleichtern. Dazu zählen für Gehörlose zahlreiche Hilfsmittel wie Schreib- und Bildtelefone, Lichtsignalanlagen oder Licht- und Vibrationsgeräte sowie die Gebärdensprache.[308] Gehörlose können zwar mittels Gebärdensprache mit anderen Menschen kommunizieren, aber auch nur wenn der Gesprächspartner ebenfalls diese Sprache beherrscht. Mit der Datenbrille könnte diese Beschränkung leicht überwunden werden. Allerdings beherrscht das Tablet „Uni“ auch die Funktion Gebärdensprache in Text zu übersetzen bzw. Text in Gebärdensprache wiederzugeben.[309] Der Vorteil bei Google Glass liegt darin mit dem Gegenüber kommunizieren zu können, ohne das Tablet in die Hand nehmen zu müssen und so gleichzeitig Augenkontakt zum Gesprächspartner halten zu können. Eine solche Unterhaltung würde demnach einer natürlichen Unterhaltung am nächsten kommen. Im Hinblick auf die Gefährdung des informationellen Selbstbestimmungsrechts stellt das Tablet jedoch eine mildere, gleich effektive Alternative zu Google Glass dar. Die

[307] Kap. 3.4.
[308] *Deutscher Gehörlosen-Bund e. V.,* Technische Hilfsmittel für Gehörlose, Internetquelle.
[309] MotionSavvy UNI, Internetquelle.

Kamera des Tablets muss gezielt auf die Hände gerichtet sein, um die Gebärdensprache in Text zu übersetzen, sodass nicht wie bei Google Glass eine unberechenbare und unsichtbare Videoaufnahme von der gesamten Person erfolgen kann. Unter diesen Umständen ist die Nutzung von Google Glass zur Übersetzung von Gebärdensprache grundsätzlich als nicht erforderlich anzusehen.

Menschen, die an Autismus leiden, haben häufig erhebliche Probleme mit anderen zu kommunizieren, insbesondere den Gesprächspartner in seiner Gestik und Mimik richtig zu deuten. Um die Kommunikationsfähigkeit zu fördern, gibt es bereits Hilfsmittel wie Smartphone Apps, die Autisten die Kommunikation durch Bilder erleichtern, indem einzelne Worte durch Bilder ersetzt und durch das Zusammenfügen Sätze gebildet werden können.[310] Dies sind geeignete mildere Mittel bei der Sprachausgabe, jedoch sind die bisherigen Hilfsmittel nicht in der Lage die Gestik und Mimik des Kommunikationspartners in einer Weise so zu interpretieren wie es mit Google Glass möglich wäre.[311] Zudem erleichtert Google Glass gleichzeitig die Pflege, den Umgang sowie die Unterstützung durch die Angehörigen. Verständnisprobleme könnten vermieden und eine angemessene kommunikative Basis für beide Seiten geschaffen werden. Unter Berücksichtigung des jeweiligen Einzelfalls könnten diese Menschen durch Google Glass eine Aufwertung ihrer Lebenssituation erhalten, sodass die Datenbrille zur Erfüllung dieses Interesses als erforderlich gesehen werden könnte.

Ferner können körperlich beeinträchtigte oder gelähmte Menschen mit Hilfe der Sprachsteuerung freien Zugang zum Internet erhalten, telefonieren und durch Sprachnachrichten mit anderen Menschen kommunizieren sowie selbst Fotos bzw. Videos anfertigen, da sie ihre Arme und Hände nicht benötigen, um ihre Motive anzuvisieren. Doch auch dieses Interesse muss sich als erforderlich erweisen. Durch die

310 *Lormis*, App hilft Autisten bei der Kommunikation, Internetquelle.
311 *Anthony*, Real-time emotion detection with Google Glass, Internetquelle.

fortschreitende technische Entwicklung von Smartphones und Smartwatches ist es bereits möglich diese teilweise per Sprachbefehl zu steuern und so im Internet surfen zu können.[312] Dennoch würde mit Google Glass die Bedienung einfacher und effektiver, sodass sich Google Glass im Einzelfall als erforderlich erweisen könnte. Zudem stellt das Szenario 3.3 kein abschließendes Bild dar. Im Gegenteil, Google Glass könnte sich bei weiteren körperlichen oder geistigen Beeinträchtigungen durchaus als erforderliche Stütze im Alltagsleben dieser Menschen erweisen.

Ein milderes Mittel könnte aber grundsätzlich darin bestehen, die Nutzung von Google Glass bzw. die zwingende Anbindung an die Google Infrastruktur zu beschränken. Für das Recht auf informationelle Selbstbestimmung ergibt sich eine zusätzliche Belastung, sobald die erfassten personenbezogenen Daten an Google und ggf. außerhalb Deutschlands, der EU oder des Europäischen Wirtschaftsraums (EWR) und damit außerhalb des Geltungsbereichs des BDSG bzw. der DSRL übermittelt werden sollen.[313] Gleiches ist für die Speicherung auf den Google-Servern anzunehmen. Es wäre ausreichend, wenn die Anwendungen in Echtzeit erfolgen und nach Gebrauch ohne Speicherung direkt gelöscht würden bzw. nur eine Speicherung auf Google Glass selbst stattfände. Demzufolge müsste die technische Ausgestaltung angepasst werden, sodass Google Glass auch in dieser beschränkten Variante genutzt werden könnte. Fraglich ist allerdings, ob solche Beschränkungen eine sinnvolle und zumutbare Alternative darstellen und somit den Zweck des Datenumgangs in vergleichbarem Maße fördern.[314] Die Erreichung des gewünschten Zwecks des Datenumgangs könnte eingeschränkt sein, da Google Glass lediglich in vollem Umfang funktioniert, wenn sie an die Google-Infrastruktur angebunden ist. Dies gehört zum Geschäftsmodell sowie zur Funktionsfähigkeit und ist für die Nutzung in diesem Umfang unentbehr-

312 Siehe z. B. Google Now, Internetquelle.
313 Vgl. Cloud Computing, *Kroschwald*, Informationelle Selbstbestimmung in der Cloud, S. 213 ff.
314 *Gola/Schomerus*, § 28 BSDG, Rn. 15.

lich. Durch diese Beschränkung wäre es den Glass-Trägern nicht möglich die aufgeführten Interessen in angemessener Weise zu erfüllen. Somit könnte unter Berücksichtigung der genannten Umstände Google Glass zur Wahrung der genannten berechtigten Interessen erforderlich sein.

6.2.1.2.2.2 Interessenabwägung

Soweit ein Datenumgang des Glass-Trägers erforderlich ist, ist zu prüfen, ob es entgegenstehende schutzwürdige Interessen gibt, die den berechtigten Interessen der verantwortlichen Stelle vorgehen. Wie die obigen Ausführungen zeigen, liegt durch die Nutzung von Google Glass ein Eingriff in die informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG der Betroffenen vor, sodass an dieser Stelle eine Interessenabwägung im Einzelfall in Anlehnung an den Verhältnismäßigkeitsgrundsatz vorzunehmen ist.

Die Interessenabwägung im Rahmen des Szenarios 3.3 erweist sich durchaus als schwierig. Festzuhalten ist, dass Google Glass eine große Hilfe zur alltäglichen Lebensgestaltung für körperlich und/oder geistig beeinträchtigte Menschen bietet. Dennoch besteht die Schwierigkeit speziell darin festzustellen, ab wann ein Mensch ein solches berechtigtes und zugleich erforderliches Interesse hat. Um dies zu ermitteln, bedarf es der medizinischen Diagnose, inwiefern sich die Beeinträchtigung bzw. Behinderung eines Menschen äußert, um ein zulässiges Interesse für die Nutzung von Google Glass begründen zu können. Dies würde bei jedem Einzelnen ein ärztliches Gutachten erfordern, das prüft, ob der Patient ein berechtigtes Interesse an der Nutzung von Google Glass hätte. Die Schwierigkeit liegt insbesondere darin die Zielgruppe festzulegen, die die Datenbrille in legitimer Weise nutzen dürfte, ohne diskriminierend über die Patienten zu urteilen.[315] Infolgedessen müssten für jeden Menschen individuelle Anwendungen bestimmt werden, die sein jeweiliges Interesse befriedigen und

[315] Vgl. Art. 3 Abs. 3 S. 2 GG, *Düring/Scholz*, in: Maunz/Düring, Art. 3 GG, Rn. 176.

nicht über das berechtigte Interesse hinausgehen. Schließlich würde Google Glass nur in begrenztem Umfang dem Glass-Träger zur Verfügung stehen. Benutzt der Träger Google Glass für Zwecke, die nicht sein berechtigtes Interesse wahren, gelten für diesen ebenfalls die Maßstäbe der gesetzlichen Vorschriften.

Aufgrund der Problematik ein berechtigtes und erforderliches Interesse des Glass-Trägers für den Datenumgang sowie spezielle Glassware zu bestimmen, ist im Rahmen der Interessenabwägung das schutzwürdige Interesse der Betroffenen höher zu gewichten. Zudem würden mit Google Glass in intransparenter Weise personenbezogene Daten in Form des Abbildes, des gesprochenen Wortes und der Verhaltensweisen erfasst, die grundsätzlich schutzwürdiger zu bewerten sind als solche Daten, die Betroffene im Regelfall preisgeben, wie z. B. Angaben zur Anschrift, Titel oder Rufnummer.[316] Daneben ist auch die Art des geplanten Datenumgangs in die Interessenabwägung einzubringen. Es muss besonders berücksichtigt werden, dass der Glass-Träger die erfassten Daten nicht nur selbst speichert, sondern auch an Google übermittelt. An dieser Stelle ist wieder auf den Aspekt der mangelnden Vorhersehbarkeit künftiger Nutzung zu verweisen. Hinzu kommt die Missbrauchsgefahr der personenbezogenen Daten Dritter.[317] Unter Berücksichtigung der genannten Umstände und der hohen Eingriffsintensität in das informationelle Selbstbestimmungsrecht überwiegen die schutzwürdigen Interessen der Betroffenen gegenüber den Interessen des Glass-Trägers. Folglich lassen sich die berechtigten Interessen des Glass-Trägers aus dem Szenario 3.3 grundsätzlich nicht durch § 28 Abs. 1 S. 1 Nr. 2 BDSG rechtfertigen.

6.2.1.2.3 Allgemein zugängliche Daten

Der Datenumgang im Rahmen der Nutzung von Google Glass durch den Nutzer könnte nach § 28 Abs. 1 S. 1 Nr. 3 BDSG zulässig sein. Voraussetzung hierfür ist, dass die Daten allgemein zugänglich sind oder

316 *Tiedemann*, NJW 1981, 945 (950).
317 Kap. 3.5 und 4.3.

die verantwortliche Stelle sie veröffentlichen dürfte, ohne das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegen.

Diese Vorschrift ist eine Konsequenz des Grundrechts auf Informationsfreiheit des Art. 5 Abs. 1 S. 1 GG.[318] Allgemein zugängliche Daten enthalten Angaben, die regelmäßig Grundlage für die Erlangung freier Information sind.[319] Darunter fallen Daten, die sich sowohl ihrer Zielsetzung als auch ihrer Publikationsform nach dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln.[320] Somit sind personenbezogene Daten dann allgemein zugänglich, wenn der Zugriff auf diese Daten für jeden rechtlich voraussetzungslos und ohne technische Zugangsbarrieren möglich ist.[321] Zu allgemein zugänglichen Quellen gehören z. B. Zeitungen, Zeitschriften, Informationsdienste, Rundfunk, Fernsehen, Telefonbücher, Bücher, öffentliche Mitteilungen im Internet sowie Informationen von Messen, Ausstellungen und Informationsständen.[322]

§ 28 Abs. 1 S. 1 Nr. 3 BDSG erleichtert zwar den Zugang zu allgemein zugänglichen Daten, die veröffentlicht werden dürfen, gibt aber die Verwendung nicht frei.[323] Die verantwortliche Stelle muss ebenfalls hinsichtlich der Interessenabwägung auf die Interessen der Betroffenen Rücksicht nehmen. Die Anforderungen daran sind jedoch wesentlich geringer als bei § 28 Abs. 1 S. 1 Nr. 2 BDSG. Da es sich um allgemein zugängliche Angaben handelt, geht der Gesetzgeber davon aus, dass ihre Verwendung den Belangen der Betroffenen grundsätzlich

318 Vgl. *Gola/Schomerus*, § 28 BDSG, Rn. 32; *Schaffland/Wiltfang*, § 28 BDSG, Rn. 133; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 57; *Plath*, in: Plath, § 28 BDSG, Rn. 76.

319 *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 259.

320 Vgl. BVerfGE 27, 71 (83); BVerfGE 33, 52 (65); siehe auch § 10 Abs. 5 S. 2 BDSG.

321 *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 81; *Hoeren*, in: Roßnagel, Hdb DS, 4.6, Rn. 34 ff.

322 *Simitis*, in: Simitis, § 28 BDSG, Rn. 51; *Gola/Schomerus*, § 28 BDSG, Rn. 32; *Plath*, in: Plath, § 28 BDSG, Rn. 76.

323 *Simitis*, in: Simitis, § 28 BDSG, Rn. 162.

nicht widerspricht.[324] Die verantwortliche Stelle darf daher die Daten so lange verwenden, wie schutzwürdige Interessen der Betroffenen, die der Verwendung entgegenstehen, nicht „offensichtlich" überwiegen.[325] In diesem Zusammenhang bedeutet die Offensichtlichkeit, dass die Verletzung der Interessen eines Betroffenen für einen unvoreingenommenen, verständigen Beobachter ohne weiteres zu erkennen ist. Eine intensive Einzelprüfung soll hingegen nicht notwendig sein, es sei denn, dass ein schutzwürdiges Gegeninteresse als Möglichkeit klar auf der Hand liegt.[326]

Es ist nun zu prüfen, ob die vom Glass-Träger in alltäglichen Situationen erfassten Daten als allgemein zugänglich anzusehen sind. In Szenario 3.1, 3.2 und 3.3 bewegt sich der Glass-Träger vorwiegend in der Öffentlichkeit, sei es auf der öffentlichen Straße oder auch innerhalb von Privatgrundstücken und Räumlichkeiten, die dem Publikumsverkehr gewidmet sind,[327] und kann dort jederzeit personenbezogene Daten erheben und verarbeiten. Fraglich ist, ob es sich hierbei um allgemein zugängliche Daten i. S. v. § 28 Abs. 1 S. 1 Nr. 3 BDSG handelt.

Den Glass-Trägern ist es, wie im Fall Google Street View gleichermaßen möglich mit der Kamera vor dem Auge in der Öffentlichkeit das Straßenbild und die sich dort aufhaltenden Personen zu erfassen. Im Rahmen von Google Street View sind sich Rechtsprechung und Literatur darüber einig, dass es sich bei der Aufnahme des Straßenbildes anfallenden Daten um allgemein zugängliche Daten i. S. d. § 28 Abs. 1 S. 1 Nr. 3 BDSG handelt und erklären Google Street View unter datenschutzrechtlichen Gesichtspunkten als zulässig.[328] Begründet wird dies damit, dass die Aufnahmen von Google vom öffentli-

---

324 *Simitis*, in: Simitis, § 28 BDSG, Rn. 162; *Gola/Schomerus*, § 28 BDSG, Rn. 31.

325 *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 267; *Simitis*, in: Simitis, § 28 BDSG, Rn. 162.

326 *Gola/Schomerus*, § 28 BDSG, Rn. 31; *Plath*, in: Plath, § 28 BDSG, Rn. 82; *Simitis*, in: Simitis, § 28 BDSG, Rn. 162 f.; *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 251; *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 103.

327 *Gola/Schomerus*, § 28 BDSG, Rn. 32; *Schwenke*, K&R 2013, 685 (690).

328 *Forgó/Krügel/Müllenbach*, CR 2010, 616 (620 f.); *Jahn/Striezel*, K&R 2009, 753 (756); *Lindner*, ZUM 2010, 292 (301); *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 84.

chen Straßenraum aus angefertigt werden, so wie dies auch jedem anderen Autofahrer oder Passanten möglich wäre.[329] Ziel des Online-Dienstes Google Street View ist es eine 360-Grad-Panorama-Straßenansicht anzubieten.[330] Dabei sollen hauptsächlich Gebäudeansichten, Straßenszenen mit Passanten sowie der Straßenverkehr abgebildet gezeigt werden, wobei Gesichter und Kfz-Kennzeichen verpixelt werden.[331]

Der Glass-Träger nimmt ebenfalls aus der Passanten-Sicht Daten in der Öffentlichkeit auf. Jedoch sind Aufnahmen von Gebäuden oder Straßenansichten eher nebensächlich.[332] In allen beschriebenen Szenarien begegnet der Glass-Träger zwangsläufig anderen Menschen, die gleichzeitig von der Datenbrille erfasst werden können. Der Glass-Träger könnte folglich im Laufe seines Alltags zahlreiche personenbezogene Daten von verschiedenen Personen erfassen. Zudem erfolgt die Aufnahme i. d. R. unbemerkt und damit unkontrolliert. Mithin handelt es sich um eine anlasslose Erhebung ohne vorherigen Kontakt. Gleichfalls besteht die Möglichkeit, dass Millionen Internetnutzer Kenntnis davon erlangen und somit eine andere Eingriffstiefe anzunehmen ist, als wenn wenige körperlich anwesende Passanten von der identischen Information Kenntnis erlangen.[333] Daneben hat das BVerfG betont, dass die hohe Streubreite eines Eingriffs, d. h. die Zahl der Grundrechtsträger, die einem Eingriff ausgesetzt sein können, gleichzeitig die Eingriffsintensität erhöht.[334] Bewegt sich der Glass-Träger als Passant im öffentlichen Raum, sind die von Google Glass erfassten personenbezogenen Aufnahmen nicht als allgemein zugängliche Daten zu rechtfertigen.[335] Die Aufnahme durch Google Glass greift in tiefster Weise in das Recht auf informationelle Selbstbestim-

[329] *Caspar*, DÖV 2009, 965 (971); *Forgó/Krügel/Müllenbach*, CR 2010, 616 (620); *Taeger*, in: Taeger/Gabel, § 28 BDSG, Rn. 84; *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 269.
[330] Google Street View, Internetquelle.
[331] *Klas*, Grenzen der Erhebung und Speicherung allgemein zugänglicher Daten, S. 50.
[332] Vgl. Kap. 6.2.1.1.
[333] *Klas*, Grenzen der Erhebung und Speicherung allgemein zugänglicher Daten, S. 50.
[334] BVerfGE 115, 320 (347).
[335] A. A. *Schwenke*, K&R 2013, 685 (689 f.).

mung des Betroffenen ein, sodass in jedem Fall das schutzwürdige Interesse des Betroffenen offensichtlich überwiegen würde. Dies lässt sich auch dadurch nicht rechtfertigen, dass es angesichts der großen Verbreitung von Digitalkameras und Smartphones sowie der Häufigkeit von Filmaufnahmen heutzutage keine Besonderheit mehr darstellt, in der Öffentlichkeit fotografiert zu werden.[336] Dementsprechend handelt es sich bei den vom Glass-Träger in der Öffentlichkeit erfassten Daten nicht um allgemein zugängliche Daten gem. § 28 Abs. 1 S. 1 Nr. 3 BDSG. Ein solcher Datenumgang des Glass-Trägers ist aus datenschutzrechtlichen Gesichtspunkten als unzulässig zu bewerten.

6.2.1.3 Rechtfertigung durch § 32 BDSG

Trägt der Beschäftigte Google Glass wie in Szenario 3.4 im Rahmen des Beschäftigungsverhältnisses, könnte die Nutzung von Google Glass gem. § 32 BDSG zulässig sein. Danach darf mit personenbezogenen Daten eines Beschäftigten nur für Zwecke des Beschäftigungsverhältnisses umgegangen werden, soweit dies für die Entscheidung über die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist oder zur Aufdeckung von Straftaten dient. Im Hinblick auf das begrenzte Ausmaß dieser Ausarbeitung beschränkt sich die Prüfung des § 32 BDSG lediglich auf die Nutzung von Google Glass am nicht-öffentlich zugänglichen Arbeitsplatz in der Logistikbranche.[337] Bezüglich der Nutzung von Google Glass bei der Polizei, im Krankenhaus und der Feuerwehr ist insbesondere auf die bereichsspezifischen Datenschutzvorschriften zu verweisen.[338]

---

336 *Forgó/Krügel/Müllenbach*, CR 2010, 616 (620).

337 Kap. 3.4.

338 Siehe zu Wearable Computing bei der Feuerwehr *Roßnagel/Jandt/Skistims/Zirfas*, Datenschutz bei Wearable Computing; BPolG sowie die Polizeigesetze der Länder, die Feuerwehrgesetze der Länder, die Krankenhausgesetze der Länder.

§ 32 BDSG soll den Beschäftigten i. S. v. § 3 Abs. 11 BDSG schützen.[339] Der Beschäftigtenbegriff ist weit gefasst und deckt sich nicht mit dem sozialversicherungsrechtlichen Begriff des Beschäftigten.[340] Demzufolge ist der Arbeitnehmer als Betroffener zu schützen, wenn er im Rahmen seines Arbeitsverhältnisses die Datenbrille trägt. Der Arbeitgeber entscheidet allein über die Mittel und Zwecke des Umgangs mit Beschäftigtendaten durch Google Glass, sodass dieser die verantwortliche Stelle gem. § 3 Abs. 7 BDSG darstellt.[341] § 32 Abs. 2 BDSG legt fest, dass der Anwendungsbereich des § 32 Abs. 1 BDSG ohne Rücksicht auf die Form der Datenspeicherung oder -übermittlung gegeben ist.[342]

Zu unterscheiden sind die zwei Zulässigkeitstatbestände des § 32 Abs. 1 BDSG. Es ist zu prüfen, unter welchen Voraussetzungen Google Glass gem. § 32 Abs. 1 S. 1 BDSG für die Durchführung des Beschäftigungsverhältnisses erforderlich ist und unter welchen Voraussetzungen Google Glass nach § 32 Abs. 1 S. 2 BDSG zur Aufdeckung von Straftaten im Beschäftigungsverhältnis eingesetzt werden könnte.

6.2.1.3.1 Google Glass zur Durchführung des Beschäftigungsverhältnisses

§ 32 Abs. 1 S. 1 BDSG erlaubt die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder

339 *Gola/Schomerus*, § 32 BDSG, Rn. 4; *Zöll*, in: Taeger/Gabel, § 32 BDSG, Rn. 1; *Seifert*, in: Simitis, § 3 BDSG, Rn. 279.

340 *Seifer*t, in: Simitis, § 32 BDSG, Rn. 12; *Däubler*, in: Däubler/Klebe/Wedde/Weichert, § 32 BDSG, Rn. 3; *Gola*, Datenschutz am Arbeitsplatz, Rn. 191; *Schreiber*, in: Plath, § 3 BDSG, Rn. 87.

341 Vgl. Kap. 6.1.3.

342 *Gola*, Datenschutz am Arbeitsplatz, Rn. 80; *Thüsing*, NZA 2009, 865 (869), *Erfurth*, NJOZ 2009, 2914 (2924); *Seifert*, in: Simitis, § 32 BDSG, Rn. 14; *Gola/Schomerus*, § 32 BDSG, Rn. 7; *Hilbrans*, in: Däubler/Hjort/Schubert/Wolmerath, Arbeitsrecht, § 32 BDSG, Rn. 3; *Selig*, Arbeitnehmerdatenschutz, S. 84; *Stamer/Kuhnke*, in: Plath, § 32 BDSG, Rn. 6.

Beendigung erforderlich ist. Angesichts der geschilderten Nutzung von Google Glass in der Logistikbranche,[343] beschränkt sich diese Ausarbeitung auf den Verwendungszweck der Durchführung des Arbeitsverhältnisses gem. § 32 Abs. 1 S. 1 Alt. 2 BDSG.

Zur Durchführung des Arbeitsverhältnisses bestimmt sind die personenbezogenen Daten, die der Arbeitgeber zur Erfüllung seiner Pflichten aber auch zur Wahrnehmung seiner Rechte gegenüber dem Arbeitnehmer vernünftigerweise benötigt.[344] Gestattet sind auch Maßnahmen zur Kontrolle, ob der Arbeitnehmer den geschuldeten Pflichten nachkommt.[345] Der erforderliche Umgang mit Beschäftigtendaten zur Durchführung des Beschäftigungsverhältnisses ergibt sich durch gesetzliche Vorschriften, Kollektivvereinbarungen und dem Arbeitsvertrag, die u. a. die Vergütung, Mitarbeiterbeurteilung und Leistungskontrolle des Mitarbeiters betreffen.[346]

Fraglich ist, ob im Rahmen der beschriebenen Nutzung von Google Glass im Szenario 3.4 von dem Beschäftigten überhaupt personenbezogene Daten erhoben und verarbeitet werden. Grundsätzlich soll Google Glass den Lagerarbeitern ihre Arbeitsaufträge erleichtern, indem diese in Echtzeit mit allen zusätzlichen Informationen übermittelt werden und die Arbeit freihändig und papierlos durchgeführt werden kann. Solange durch die Kamerafunktion keine personenbezogenen Daten erfasst werden und keine Verknüpfung zu Daten aus der Personalakte etc. stattfindet, werden in dieser Konstellation i. d. R. keine personenbezogenen Daten erhoben und verarbeitet. Eine solche Nutzung von Google Glass fällt demnach nicht in den Anwendungsbereich des § 32 Abs. 1 S. 1 Alt. 2 BDSG.

---

343 Kap. 3.4.

344 Es dürfen alle die Stammdaten gespeichert werden, die für den zukünftigen Verlauf des Arbeitsverhältnisses von Bedeutung werden können.

345 *Gola/Schomerus*, § 32 BDSG, Rn. 11; *Seifert*, in: Simitis, § 32 BDSG, Rn. 77; *Zöll*, in: Taeger/Gabel, § 32 BDSG, Rn. 26.

346 *Zöll*, in: Taeger/Gabel, § 32 BDSG, Rn. 28; *Däubler*, Gläserne Belegschaften?, Rn. 253; *Gola*, Datenschutz am Arbeitsplatz, Rn. 194.

Allerdings ist es vorstellbar, dass der Arbeitgeber gleichzeitig die Kamerafunktion von Google Glass, im Rahmen seinen zu der Durchführung des Arbeitsverhältnisses bestehenden Rechte, zur Kontrolle des Verhaltens und der Leistung jederzeit benutzen kann.[347] Mit Google Glass wäre es dem Arbeitgeber möglich, durch die Augen der Beschäftigten zu schauen und so deren Leistung zu überprüfen. Daher ist zu untersuchen, ob sich die Nutzung von Google Glass zur Verhaltens- und Leistungskontrolle durch § 32 Abs. 1 S. 1 Alt. 2 BDSG legitimieren lassen könnte.[348] Aufgrund der Ähnlichkeit zur Videoüberwachung, als Maßnahme der Kontrolle, ist die dazu ergangene Rechtsprechung und Literatur für die Beurteilung der Zulässigkeit heranzuziehen.[349] Maßstab für die Zulässigkeit von Bild- und Videoaufzeichnungen ist die in § 32 Abs. 1 S. 1 BDSG enthaltene Erforderlichkeit.[350] Demnach ist zu prüfen, ob Google Glass für die Durchführung des Beschäftigungsverhältnisses, d. h. zur Mitarbeiterüberwachung erforderlich ist.

Grundsätzlich ist eine Videoüberwachung unzulässig, wenn sie in die Intimsphäre von Beschäftigten eingreift.[351] Gerade weil der Arbeitgeber die Mitarbeiterüberwachung durch die Augen des Beschäftigten durchführt, dringt er in privateste oder sogar in manchen Situationen in intimste Sphären des Beschäftigten ein.[352] So ist jeder Gang zur Toilette oder das Umziehen in der betriebseigenen Umkleidekabine dem Arbeitgeber ersichtlich. Daraus ergibt sich ein Eingriff in das Recht auf informationelle Selbstbestimmung von höchster Intensität. Herkömmliche Videokameras stellen in diesem Fall ein zumutbares gleich geeignetes und weniger in das informationelle Selbstbestimmungsrecht eingreifende Mittel dar, um den Zweck der Mitarbeiterkontrolle zu er-

347 BT-Drs. 16/13657, S. 36; *Gola/Schomerus*, § 32 BDSG, Rn. 11; *Thüsing*, NZA 2009, 865 (868); *Seifert*, in: Simitis, § 32 BDSG, Rn. 77; *Däubler*, Gläserne Belegschaften?, Rn. 292.

348 *Seifert*, in: Simitis, § 32 BDSG, Rn. 80; *Gola/Schomerus*, § 32 BDSG, Rn. 11; BT-Drs. 16/13657, 36; *Erfurth*, NJOZ 2009, 2914 (2917).

349 BT-Drs. 16/13 657, 36; BAG NZA 2008, 1187; BAGE 105, 356 = NZA 2003, 1193; BAG NJW 2005, 313.

350 *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 32 BDSG, Rn. 95a; *Forst*, in: Auernhammer, § 32 BDSG, Rn. 53.

351 *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 32 BDSG, Rn. 95e.

352 *Schwenke*, K&R 2013, 685 (691).

füllen. Jedoch sind dabei die strengen Zulässigkeitsvoraussetzungen zu beachten.[353] Folglich ist die Nutzung von Google Glass zur Durchführung des Beschäftigungsverhältnisses, insbesondere der Verhaltens- und Leistungskontrolle gem. § 32 Abs. 1 S. 1 BDSG nicht zulässig. Ein Einsatz von Google Glass im Rahmen der Durchführung des Beschäftigungsverhältnisses würde sich nur unter besonderen Umständen und punktuell z. B. zu Trainingszwecken oder bei gefährlichen Einsätzen im Sicherheitsbereich rechtfertigen lassen.[354]

6.2.1.3.2 Google Glass zur Aufdeckung von Straftaten im Beschäftigungsverhältnis

Des Weiteren könnte sich die Zulässigkeit von Google Glass im Beschäftigungsverhältnis gem. § 32 Abs. 1 S. 2 BDSG ergeben, wenn die Erhebung, Verarbeitung und Nutzung personenbezogener Daten eines Beschäftigten bei der Aufdeckung von Straftaten, die im Beschäftigungsverhältnis begangen worden sind, erfolgt. § 32 Abs. 1 S. 2 BDSG ist die speziellere Norm[355] des § 32 Abs. 1 BDSG und erlaubt einen Datenumgang, sofern zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss des Datenumgangs nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Die Zulässigkeitskriterien des § 32 Abs. 1 S. 2 BDSG greifen erst, wenn der Verdacht eines strafbaren Verhaltens nachgewiesen wird. Soll dem Verdacht nun zielgerichtet nachgegangen werden, was regelmäßig durch heimliche Beobachtung geschieht, sind die Anforderungen des

---

353 Siehe dazu *Seifert*, in: Simitis, § 32 BDSG, Rn. 78 ff., *Gola/Schomerus*, § 32 BDSG, Rn. 19; *v. Zezschwitz*, in: Roßnagel, Hdb DS, 9.3; *Thüsing/Pötters*, in: Thüsing (Hrsg.), Beschäftigtendatenschutz und Compliance, § 11.

354 So *Schwenke*, K&R 2013, 685 (691).

355 *Erfurth*, NJOZ 2009, 2914 (2920); *Schmidt*, DuD 2010, 207 (210).

§ 32 Abs. 1 S. 2 BDSG zu erfüllen.[356] Die Intensität der Überwachungsmaßnahme ist an dem Gewicht der Straftat zu messen.[357] Weiterhin muss die (verdeckte) Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten zur Aufdeckung der Straftat auch erforderlich sein. Es ist im Einzelfall zu prüfen, ob die Aufklärung der Straftat auch mit weniger intensiven Eingriffen in die informationelle Selbstbestimmung des oder der betroffenen Beschäftigten erfolgen kann.[358]

Zunächst ist zu untersuchen, inwiefern sich Google Glass eignet und erforderlich ist, um Straftaten von Beschäftigten aufzudecken. Die Datenbrille kann zwar auch als Überwachungsmedium genutzt werden, allerdings ist diese nicht dafür ausgelegt und aufgrund beschränkter Akkulaufzeit und subjektiver Aufnahme durch die Augen eines Beschäftigten ungeeignet, um bereits begangene Straftaten aufzudecken.[359] Zielt der Arbeitgeber darauf ab, durch den Blick des Beschäftigten andere Mitarbeiter zu überwachen erfolgt die Überwachung sehr subjektiv, da ihm nur das Bild zukommt, das sich im Blickfeld des Glass-Trägers befindet. Durch diese einseitige und subjektive Überwachung wird es fast nicht möglich sein, konkrete Straftaten aufzudecken. In diesem Fall stellt Google Glass kein geeignetes Mittel zur Zweckerreichung dar. Besteht ein konkreter Verdacht gegen den Glass-Träger, könnte Google Glass wiederum geeignet sein, da die Datenbrille die Straftat unmittelbar aus dem Blickfeld des Täters aufnimmt. Allerdings wird eine solche intensive Überwachungsmaßnahme in keinem Fall erforderlich sein. Mithin ist die Intensität des Eingriffs in die informationelle Selbstbestimmung i. d. R. stärker als die Schwere der Straftat zu gewichten. Ein solch intimer Eingriff in das Recht auf informationelle Selbstbestimmung ist keineswegs erforderlich, um eine Straftat aufzudecken. Der Arbeitgeber hat vielmehr auf mildere Maßnahmen wie die herkömmliche (heimliche) Videoüber-

356 *Gola/Schomerus*, § 32 BDSG, Rn. 26.
357 *Zöll*, in: Taeger/Gabel, § 32 BDSG, Rn. 53; *Seifert*, in: Simitis, § 32 BDSG, Rn. 101; *Gola/Schomerus*, § 32 BDSG, Rn. 27.
358 *Seifert*, in: Simitis, § 32 BDSG, Rn. 105.
359 Vgl. Kap. 6.2.1.1.

wachung bzw. andere Ermittlungsmaßnahmen wie die Mitarbeiterbefragung zurückzugreifen.[360] Demzufolge ist die Nutzung von Google Glass zur Aufdeckung von Straftaten im Beschäftigungsverhältnis gem. § 32 Abs. 1 S. 2 BDSG unzulässig.

6.2.1.3.3 Mitbestimmung des Betriebsrats und Personalrats

Die Vorschrift des § 32 Abs. 3 BDSG knüpft an den bereits bestehenden kollektivrechtlichen Beschäftigtendatenschutz an und stellt klar, dass die Beteiligungsrechte der Interessenvertretungen unberührt bleiben. Die Schutzvorschriften des § 32 Abs. 1 und 2 BDSG und die Vorschriften des Arbeitnehmerdatenschutzes im kollektiven Arbeitsrecht treten somit in ein Komplementärverhältnis.[361] Sofern in einem Unternehmen ein Betriebsrat bzw. Personalrat besteht, sind aufgrund des Verwendungszwecks der Verhaltens- und Leistungskontrolle an dieser Stelle auch die zwingenden Mitbestimmungsrechte des Betriebsrats und Personalrats nach § 87 Abs. 1 Betriebsverfassungsgesetz (BetrVG) und § 75 Bundespersonal-vertretungsgesetz (BPersVG) zu beachten. Beim Umgang mit Google Glass sind bzgl. der Wahrung von Persönlichkeitsrechten der Beschäftigten § 87 Abs. 1 Nr. 6 BetrVG und § 75 Abs. 3 Nr. 17 BPersVG einschlägig.[362] Danach haben der Betriebsrat und der Personalrat mitzubestimmen, wenn es um die Einführung und Anwendung von technischen Einrichtungen geht, die dazu bestimmt sind, Rückschlüsse auf das Verhalten oder die Leistung betroffener Arbeitnehmer zu geben. Maßgeblich dabei ist nicht der mit Google Glass verfolgte Zweck, sondern allein der Umstand, dass die Anwendung objektiv zur Überwachung der Mitarbeiter geeignet ist.[363] In Anlehnung an die Funktionsweise herkömmlicher Videokameras erfüllt auch Google Glass die Tatbestandsmerkmale des § 87 Abs. 1 Nr. 6 BetrVG und des

360 *Maschmann*, NZA-Beil. 2012, 50 (55).
361 *Seifert*, in: Simitis, § 32 BDSG, Rn. 145.
362 *Kania*, in: ErfK, § 75 BetrVG, Rn. 9; *Richardi*, in: Richardi, § 87 BetrVG, Rn. 478; *Kaiser*, in: Richardi/Dörner/Weber, § 75 BPersVG, Rn. 532 ff.
363 BAG, NJW 1980, 359.

§ 75 Abs. 3 Nr. 17 BPersVG.[364] Zudem sind der Arbeitgeber und Betriebsrat daran gehalten gem. § 75 Abs. 2 S. 1 BetrVG die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Durch dieses betriebsverfassungsrechtliche Übermaßgebot sollen gerade rechtswidrige Verletzungen des Persönlichkeitsrechts verhindert werden.[365] Unter Berücksichtigung dieses Übermaßgebots ist Google Glass zur Verhaltens- und Leistungskontrolle unter Mitbestimmung des Betriebs- und Personalrats als unzulässig zu bewerten.[366]

6.2.1.4 Einwilligung als Legitimation

Neben einer Rechtsvorschrift als Erlaubnistatbestand sieht § 4 Abs. 1 BDSG für die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten auch die Einwilligung des Betroffenen vor. Im BDSG sind die Voraussetzungen für eine wirksame Einwilligung u. a. in § 4a BDSG geregelt. Die bereichsspezifische Vorschrift zur Einwilligung des § 22 S. 1 KUG zur Verbreitung und öffentlichen Zurschaustellung von Bildern[367] verdrängt § 4a BDSG. Angesichts des datenschutzrechtlichen Schwerpunkts der Arbeit liegt jedoch die datenschutzrechtliche Einwilligung des § 4a BDSG im Fokus. Demnach ist zu prüfen, ob die Einwilligung der Betroffenen die Verwendung personenbezogener Daten des Glass-Trägers rechtfertigen könnte.[368] Mit der Einwilligung, als Ausdruck des informationellen Selbstbestimmungsrechts entscheidet der Betroffene, ob und unter welchen Bedingungen mit seinen personenbezogenen Daten umgegangen werden darf.[369] Die inhaltlichen und formalen Voraussetzun-

[364] Vgl. zur Videoüberwachung schon BAG, NJW 2003, 3436 = NZA 2003, 1193; *Tammen*, RDV 2000, 15.

[365] *Fitting*, § 75 BetrVG, Rn. 136 ff.

[366] In der notwendigen Betriebsvereinbarung kann die datenschutzrechtliche Gestaltung der Anwendung geregelt werden.

[367] Die Einwilligung ist nur wirksam, wenn der jeweiligen Person die Art, der Umfang und der Zweck der Zurschaustellung bekannt sind, siehe *Dreier/Specht*, in: Dreier/Schulze, § 22 KUG, Rn. 17-19.

[368] *Holznagel/Sonntag*, in: Roßnagel, Hdb DS, 4.8, Rn. 24.

[369] *Simitis*, in: Simitis, § 4a BDSG, Rn. 2.

gen für eine wirksame Einwilligung bestimmen sich nach § 4a BDSG. Gemäß § 4a Abs. 1 BDSG hat sie freiwillig, informiert und schriftlich zu erfolgen.[370]

Eine Einwilligung im Rahmen von Google Glass kommt als Erklärung eines betroffenen Dritten gegenüber dem Glass-Träger in Betracht. Zweifelhaft ist jedoch, ob die Einwilligung zur Legitimierung des Umgangs personenbezogener Daten sinnvoll erscheint. Gerade im Bereich des Ubiquitous Computing sowie des Wearable Computing stößt die Einwilligung an ihre Grenzen.[371] Es ist davon auszugehen, dass ein Glass-Träger im Laufe seines Alltags vielen Menschen begegnet und unbemerkt personenbezogene Daten Dritter erheben könnte. Um den Umgang mit Betroffenendaten zu legitimieren, müsste für jeden Akt der Erhebung, Verarbeitung und Nutzung eine Einwilligung des Betroffenen gegeben werden. Hinzu kommen die Masse und Vielfalt verschiedener Anwendungen und die für die jeweiligen Phasen und Zwecke des Datenumgangs verantwortliche Stellen. Schließlich würde es unter den genannten Umständen zu einer Überforderung aller Beteiligten führen, sodass die Einwilligung kein angemessenes Mittel darstellt, um den Datenumgang zu legitimieren.[372]

Bei der Nutzung von Google Glass am Arbeitsplatz ist die Einwilligung als Legitimation des Datenumgangs ebenfalls fragwürdig. Zweifel bestehen bereits bei der in § 4a Abs. 1 S. 1 BDSG geforderten Freiwilligkeit der datenschutzrechtlichen Einwilligung, da sich Arbeitgeber und Arbeitnehmer in einem ungleichen Machtverhältnis befinden.[373] Um dies festzustellen, bedarf es einer Einzelfallprüfung. Im Regelfall spricht aber eine Vermutung dafür, dass eine gegenüber dem

370 *Plath*, in: Plath,§ 4a BDSG, Rn. 12, 23; *Bergmann/Möhrle/Herb*, § 4a BDSG, Rn. 3b; ausführlich zu den Tatbestandsmerkmalen *Simitis*, in Simitis, § 4a BDSG; *Holznagel/Sonntag*, in: Roßnagel, Hdb DS, 4.8.

371 Siehe dazu *Roßnagel/Müller*, CR 2004, 625; *Roßnagel*, MMR 2005, 71.

372 Siehe zum Ubiquitous Computing *Roßnagel*, MMR 2005, 71 (72); *Roßnagel/Müller*, CR 2004, 625 (629).

373 *Däubler*, Gläserne Belegschaft?, Rn. 136; *Büllesbach*, in: Roßnagel, Hdb DS, 6.1, Rn. 14.

Arbeitgeber abgegebene Einwilligung unfreiwillig ist.[374] Angesichts der enormen Eingriffstiefe in das informationelle Selbstbestimmungsrecht des Arbeitnehmers[375] bei der Nutzung von Google Glass ist in diesem Fall von einer unwirksamen Einwilligung auszugehen.

6.2.1.5 Zwischenfazit

Grundsätzlich scheidet die Einwilligung als Legitimationsgrundlage aus und auch die gesetzlichen Erlaubnistatbestände für den Datenumgang aus dem BDSG könnten nur vereinzelt und unter engen Voraussetzungen für beeinträchtigte Menschen eine Rechtsgrundlage für den Datenumgang durch den Glass-Träger bieten. Die zentrale Erlaubnisnorm beim Datenumgang des Glass-Trägers stellt § 28 Abs. 1 S. 1 Nr. 2 BDSG sowie in speziellen Einzelfällen im Arbeitsverhältnis § 32 Abs. 1 S. 1 BDSG dar.

6.2.2 Datenumgang durch Google

Im Folgenden wird die datenschutzrechtliche Zulässigkeit der Übermittlung und Speicherung der personenbezogenen Daten durch Google vorgenommen. Grundsätzlich ist anzunehmen, dass die maßgebliche Entscheidung über Art, Umfang und Dauer der Datenverarbeitung durch die Konzernzentralen mit Sitz in den USA und somit außerhalb des Geltungsbereichs der EU sowie nationaler Gesetzgebung getroffen werden.[376] Während in diesem Fall die Eröffnung des sachlichen Anwendungsbereichs des BDSG mit Verweis auf die Erläuterungen in Kap. 6.1 anzunehmen ist, konzentriert sich hingegen dieser Abschnitt auf den räumlichen Anwendungsbereich des BDSG. Demgemäß ist vorab festzustellen, ob der Datenumgang durch Google, mit Sitz in den USA, in den räumlichen Anwendungsbereich des BDSG fällt und infolgedessen die Zulässigkeit des Datenumgangs anhand der Vorschriften dieses Gesetzes beurteilt werden kann.

---

374 *Däubler*, in: Däubler/Klebe/Wedde/Weichert, § 4a BDSG, Rn. 23.
375 Kap. 6.2.1.3.
376 *Karg*, ZD 2013, 371.

6.2.2.1 Räumlicher Anwendungsbereich des BDSG

Um die Zulässigkeit des Datenumgangs durch Google mit Sitz in den USA anhand des BDSG beurteilen zu können, ist zunächst zu prüfen, ob in diesem Fall das deutsche Datenschutzrecht anwendbar ist. Welches Datenschutzrecht in Fällen mit Auslandsberührung anzuwenden ist, bestimmt sich nach den Kollisionsregelungen in § 1 Abs. 5 BDSG,[377] der die Vorgaben des Art. 4 DSRL umsetzt.[378]

6.2.2.1.1 Sitzland-/Niederlassungsprinzip

Grundsätzlich bestimmt sich die Anwendbarkeit des BDSG nach dem Territorialitätsprinzip, wonach jede Verwendung personenbezogener Daten innerhalb Deutschlands primär dem BDSG unterliegt.[379] Als innergemeinschaftliche Kollisionsvermeidungsnorm weicht § 1 Abs. 5 S. 1 BDSG jedoch hiervon ab, indem es für den Datenverkehr zwischen EU- oder EWR-Staaten das sog. Sitzlandprinzip vorschreibt.[380] Unabhängig vom Ort der Datenverarbeitung ist für die Anwendbarkeit des nationalen Datenschutzrechts maßgeblich, wo innerhalb der EU/EWR der Sitz der verantwortlichen Stelle liegt.[381] Insofern wird das Territorialitätsprinzip für den grenzüberschreitenden Datentransfer innerhalb der EU/EWR aufgehoben.[382] Demzufolge verzichtet der jeweilige Mitgliedstaat, in diesem Falle Deutschland, auf die Anwendung seiner Regelungen auf Datenaktivitäten im Inland, sofern sie von einer Stelle mit Sitz in einem anderen Mitgliedstaat ausgeführt werden. Dadurch soll in erster Linie neben der Stär-

---

377 § 1 Abs. 5 BDSG verdrängt als lex specialis die allgemeinen Kollisionsnormen der Art. 3-46a EGBGB, sowie die Rom II Verordnung.

378 *Bergmann/Möhrle/Herb*, § 4b BDSG, Rn. 10.

379 *v. Lewinski*, in: Auernhammer, § 1 BDSG, Rn. 46; *Jotzo*, MMR 2009, 232; BT-Drs. 14/4329, 31; *Voigt*, ZD 2014, 15 (16).

380 BT-Drs. 14/4329, S. 31; *Dammann*, in: Simitis, § 1 BDSG, Rn. 198 ff.; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 1 BDSG, Rn. 16; *Dammann*, RDV 2002, 70.

381 *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 49; *Plath*, in: Plath, § 1 BDSG, Rn. 45; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 1 BDSG, Rn. 15; *Gola/Schomerus*, § 1 BDSG, Rn. 27; *Dammann*, in: Simitis, § 1 BDSG, Rn. 198.

382 BT-Drs. 14/4329, S. 31; *Jotzko*, MMR 2009, 232 (235).

kung des Binnenmarkts ein einheitlicher Schutzstandard in der EU geschaffen sowie Doppelregelungen und Regelungslücken vermieden werden.[383]

Zur Wahrung der Rechte der Betroffenen schwächt § 1 Abs. 5 S. 1 2. HS BDSG das Sitzlandprinzip ab.[384] Dem Niederlassungsprinzip aus Art. 4 Abs. 1 lit. a) DSRL folgend, regelt § 1 Abs. 5 S. 1 2. HS BDSG, dass das BDSG auf Aktivitäten in einem anderen Mitgliedstaat der EU/EWR anzuwenden ist, sofern die Datenerhebung, -verarbeitung oder -nutzung durch eine Niederlassung der verantwortlichen Stelle in Deutschland erfolgt.[385] Ebenso ist bei Datenverarbeitungen durch verantwortliche Stellen mit Sitz in einem Drittland, also außerhalb der EU/EWR wesentlich, ob die Verarbeitung durch die ausländische verantwortliche Stelle selbst oder durch eine deutsche bzw. europäische Niederlassung stattfindet.[386] Demnach ist das deutsche Datenschutzrecht anzuwenden, soweit eine Datenverarbeitung im Inland durch eine in Deutschland ansässige Niederlassung erfolgt.[387] § 1 Abs. 5 S. 1 BDSG unterscheidet zwischen der Niederlassung in der EU/EWR und dem für die Verarbeitung Verantwortlichen. Demnach kommt das Recht der EU/EWR Mitgliedstaates zur Anwendung, in dem eine Niederlassung des für die Verarbeitung Verantwortlichen, an Datenverarbeitungstätigkeiten beteiligt ist.[388] Weder das BDSG noch die DSRL statuieren ein Konzernprivileg, wonach ein Konzern als eine einheitliche Stelle gem. § 3 Abs. 7 BDSG behandelt wird.[389] Diesbezüglich sind die Niederlassungen in der

383 *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 54; *Dammann,* in: Simitis, § 1 BDSG, Rn. 199; *Plath*, in: Plath, § 1 BDSG, Rn. 46; *Jotzo,* MMR 2009, 232 (235); siehe auch Erwägungsgrund 7 f. DSRL.

384 *Dammann*, in: Simitis, § 1 BDSG, Rn. 199; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 55.

385 *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 55.

386 *Voigt*, ZD 2014, 15 (17).

387 *Dammann*, in: Simitis, § 1 BDSG, Rn. 199; *Gola/Schomerus*, § 1 BDSG, Rn. 28; *Jotzo,* MMR 2009, 232 (234 ff.).

388 Art. 29 Datenschutzgruppe, WP 179, S. 14 ff.

389 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 3 BDSG, Rn. 59; *Scheja*, Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank, S. 68 ff., *Pauly/Ritzer/Geppert*, ZD 2013, 423 (425).

EU/EWR und der für die Verarbeitung Verantwortliche als zwei getrennte Stellen zu betrachten und voneinander abzugrenzen.[390]

6.2.2.1.2 Territorialitätsprinzip

In Umsetzung von Art. 4 Abs. 1 lit. c) DSRL gilt bezüglich der Anwendbarkeit des BDSG bei grenzüberschreitenden Sachverhalten für verantwortliche Stellen, die nicht in einem Mitgliedstaat der EU/EWR belegen sind und personenbezogene Daten im Inland erheben, verarbeiten und nutzen, das Territorialitätsprinzip gem. § 1 Abs. 5 S. 2 BDSG.[391] Diese Regelung dient in erster Linie dem Schutz des Betroffenen. Dadurch wird verhindert, dass möglicherweise ein geringerer als der durch die DSRL etablierte Datenschutzstandard in der EU/EWR zur Geltung kommt, soweit verantwortliche Stellen, die in einem Drittland gelegen sind, personenbezogene Daten innerhalb der EU/EWR erheben, verarbeiten und nutzen.[392] Allerdings reicht der Schutz der DSRL weiter als die Formulierung des § 1 Abs. 5 S. 2 BDSG, woraufhin das nationale Recht soweit wie möglich richtlinienkonform auszulegen ist.[393] Dementsprechend wird, in Anlehnung an Art. 4 Abs. 1 lit. c) DSRL, neben dem Datenumgang im Inland verlangt, dass die verantwortliche Stelle zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreifen muss, die im Hoheitsgebiet des betreffenden Mitgliedstaats gelegen sind.[394] Dadurch wird der Schutz insbesondere im Hinblick auf automatisierte Verarbeitung durch fremdgesteuerte Anlagen erweitert.[395]

---

390 OVG Schleswig, ZD 2013, 364 (365); *Buchner*, in: Taeger/Gabel, § 3 BDSG, Rn. 53.

391 *Gola/ Schomerus*, § 1 BDSG, Rn. 27 ff.; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 1 BDSG, Rn. 17a.

392 BT-Drs. 14/4329, S. 31; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 57; *Dammann*, in: Simitis, § 1 BDSG, Rn. 214; *Dammann*, RDV 2002, 70 (73).

393 *Ruffert*, in: Calliess/Ruffert, Art. 288 AEUV, Rn. 77 ff., *Nettesheim*, in: Grabitz/Hilff/Nettesheim, Art. 288 AEUV, Rn. 133 ff.; *Plath*, in: Plath § 1 BDSG, Rn. 62; *Gabel*, in: Taeger/Gabel, § 1 BDSG, Rn. 58; *Dammann*, in: Simitis, § 1 BDSG, Rn. 218; *Karg*, ZD 2013, 371 (373).

394 Ausführlich zum Rückgriff auf Mittel *Dammann*, in: Simitis, § 1 BDSG, Rn. 214 ff.

395 *Dammann*, in: Simitis, § 1 BDSG, Rn. 219.

6.2.2.1.3 Datenumgang durch Google im Rahmen einer Niederlassung

Das BDSG könnte auf den Datenumgang durch Google gem. § 1 Abs. 5 S. 1 2. HS BDSG anwendbar sein, soweit die Übermittlung und Speicherung der personenbezogenen Daten in Deutschland durch eine hier ansässige Niederlassung erfolgt.

Umstritten ist, wann eine Niederlassung i. S. v. § 1 Abs. 5 S. 1 BDSG vorliegt, denn die DSRL und das BDSG definieren diesen Begriff nicht.[396] Anhaltspunkt für die Terminologie der Niederlassung ist der Erwägungsgrund 19 DSRL, wonach eine Niederlassung im Hoheitsgebiet eines Mitgliedstaats eine effektive und tatsächliche Ausübung der Tätigkeit mittels einer festen Einrichtung voraussetzt, unabhängig von der gewählten Rechtsform einer solchen Niederlassung.[397] Nicht vom Begriff der Niederlassung erfasst sind nur vorübergehend angelegte Aktivitäten wie z. B. das Unterhalten eines Messestandes sowie mangels effektiver Tätigkeitsausübung Briefkastenfirmen oder ein bloßer Rechner- oder Serverstandort.[398] Maßgeblich für den Begriff der datenschutzrechtlich relevanten Niederlassung ist mittels einer richtlinienkonformen Auslegung des § 1 Abs. 5 S. 1 BDSG anhand von Art. 4 Abs. 1 lit. a) DSRL, dass die Verarbeitung personenbezogener Daten in Deutschland im Rahmen der Tätigkeit einer Niederlassung ausgeführt wird. Es kommt hingegen nicht darauf an, ob die Niederlassung die personenbezogenen Daten tatsächlich verarbeitet.[399] In diesem Zusammenhang ist fraglich, in welchem Fall eine Niederlassung eine Tätigkeit effektiv und tatsächlich ausübt.[400] Dazu ist das

396 Art. 29-Datenschutzgruppe, WP 179, S. 14.

397 *Weichert*, in: Däubler/Klebe/Wedde/Weichert, § 1 BDSG, Rn. 17; überwiegend wird auf die Begriffsbestimmung des § 4 Abs. 3 GewO zurückgegriffen.

398 Art. 29-Datenschutzgruppe, WP 56, S. 9, WP 179, S. 15; OVG Schleswig NJW 2013, 1977, *Scheja,* Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank, S. 83 f.; *Dammann*, in: Simitis, § 1 BDSG, Rn. 203; a. A. *Bergmann/Möhrle/Herb*, § 1 BDSG, Rn. 43.

399 Art. 29-Datenschutzgruppe, WP 179, S. 14 ff.

400 Hierzu *Pauly/Ritzert/Geppert*, ZD 2013, 423.

Vorgehen des Datenumgangs für einzelne Tätigkeiten zu untersuchen und zu bestimmen, ob die jeweilig untersuchte Niederlassung hieran beteiligt ist.[401]

Bisher wurde eine wesentliche Teilnahme am jeweiligen Datenumgang gefordert, um für diesen im Einzelnen eine Aktivität im Rahmen der Tätigkeit der Niederlassung zu begründen.[402] So entschied das OVG Schleswig im April 2013, dass eine Niederlassung nur dann eine datenschutzrechtlich verantwortliche Stelle sei, wenn sie die von der DSRL geforderte Kompetenz aufweise, über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten zu entscheiden.[403]

Allerdings dürfte seit dem Urteil des EuGHs vom 13.05.2014 zum Anspruch auf Datenlöschung gegenüber Google[404] die Rechtslage anders zu bewerten sein. Die Entscheidung des EuGH setzt dahingehend neue Maßstäbe für das europäische und infolgedessen auch für das deutsche Datenschutzrecht. Die neuen Maßstäbe müssen bei der datenschutzrechtlichen Beurteilung von Google Glass herangezogen werden. Dem EuGH zufolge sei deutsches Datenschutzrecht anzuwenden, wenn eine Niederlassung in Deutschland als für die Datenverarbeitung verantwortliche Stelle anzusehen ist. Demnach würde für das Unternehmen Google, das auf dem europäischen Markt agiert, aufgrund seiner Niederlassungen in Deutschland deutsches Datenschutzrecht gelten.[405] Um dementsprechend die Anwendbarkeit des BDSG für den Datenumgang von Google zu bejahen, müsste der Datenumgang der personenbezogenen Daten im „Rahmen der Tätigkeit" einer Niederlassung in Deutschland erfolgen. Der EuGH differenziert in seiner Argumentation sehr genau und stellt darauf ab, dass die Datenverarbeitung nicht „von", sondern nur „im Rahmen" der Aktivitä-

401 Ausführlich Art. 29-Datenschutzgruppe, WP 179, S. 16 ff.
402 *Karg*, ZD 2013, 375; *Polenz*, VuR 2012, 207 (208 ff.); *Steinrötter*, MMR 2013, 691 ff.; OVG Schleswig, NJW 2013, 1978; a. A. OLG Hamburg ZD 2011, 138 und LG Berlin BeckRS 2013, 08005.
403 OVG Schleswig, ZD 2013, 364 ff.; Vorinstanz VG Schleswig, ZD 2013, 245.
404 EuGH, Urteil v. 13.05.2014 – C-131/12.
405 EuGH, Urteil v. 13.05.2014 – C-131/12, Rn. 45 ff.

ten der Niederlassung durchgeführt werden müsse.[406] Das bedeutet, dass die Niederlassung in Deutschland nicht selbst die Datenverarbeitung ausführen muss, sondern es ausreichend ist, wenn die Datenverarbeitung in Bezug auf die Aktivitäten dieser Niederlassung durchgeführt wird.[407] Die Niederlassungen von Google in Deutschland arbeiten an der Entwicklung globaler Produkte und IT-Leistungen und gestalten den Vertrieb sowie das Marketing des Unternehmens.[408] Im Rahmen ihrer Tätigkeit greifen sie zwangsläufig auf die unternehmenseigenen Server zurück, auf welchen die vom Glass-Träger erfassten Daten gespeichert sind. Die Tätigkeiten der Niederlassungen könnten angesichts der Gestaltung des Geschäftsmodells, welches u. a. in der Bereitstellung und Fortentwicklung der Glassware liegt, eng mit der Tätigkeit von Google Inc. verbunden sein. Hinzu kommt die generelle finanziell nützliche, administrative und unterstützende Tätigkeit der Niederlassungen, die mit der eigentlich durch den Hauptsitz durchgeführten Datenverarbeitung in Verbindung steht.[409] Ebenso ist unerheblich, an welchem Standort sich die unternehmenseigenen Server befinden.[410] Im Hinblick auf das weite Verständnis des EuGHs zur Verantwortlichkeit einer Niederlassung, ist somit davon auszugehen, dass die deutschen Niederlassungen dementsprechend tätig sind.[411] Dies hat zur Folge, dass für das Übermitteln und Speichern auf die Google Server die deutschen Niederlassungen des US-Unternehmens verantwortlich sind. Gem. § 1 Abs. 5 S. 1 2. HS BDSG ist das deutsche Datenschutzrecht auf den Datenumgang durch Google anzuwenden.

Die Regel des § 1 Abs. 5 S. 2 BDSG, wonach es bei Stellen mit Sitz in Drittstaaten auf die Belegenheit der Mittel für die Bestimmung des

406 EuGH, Urteil v. 13.05.2014 – C-131/12, Rn. 52.
407 EuGH, Urteil v. 13.05.2014 – C-131/12, Rn. 52 ff.
408 Tätigkeiten der Google Niederlassungen in Hamburg, Berlin, München, Internetquelle.
409 EuGH, MMR 2014, 455 (465) m. Anm. *Sörup*; *Arning/Moos/Schefzig*, CR 2014, 447 (449 f., 455); *Karg*, ZD 2014, 359.
410 Art. 29-Datenschutzgruppe, 179, S. 16; danach erfüllen die Einrichtungen in Deutschland auch dann die beschriebenen Anforderungen, wenn sich die Server ausschließlich in den USA befänden.
411 Kritisch dazu *Arning/Moos/Schefzig*, CR 2014, 447 (450).

anwendbaren Rechts ankommt, wird in diesem Fall durch die Anwendung des Niederlassungsprinzips des § 1 Abs. 5 S. 1 2. HS BDSG verdrängt.[412]

6.2.2.2 Rechtfertigung durch § 28 BDSG

Aufgrund der Anwendbarkeit des BDSG ist zu prüfen, ob sich der Datenumgang durch Google mit den Vorschriften des BDSG rechtfertigen lassen könnte.

Grundsätzlich ist davon auszugehen, dass die Übermittlung und Speicherung der personenbezogenen Daten durch Google zur Erfüllung eigener Geschäftszwecke erfolgt und § 28 Abs. 1 S. 1 BDSG die einschlägige Norm darstellt. Danach könnte der Datenumgang durch Google zu eigenen Geschäftszwecken zulässig sein, wenn dies zur Erfüllung eines Schuldverhältnisses zwischen Google und dem Betroffenen erforderlich ist (Nr. 1), eine Übermittlung bzw. Speicherung nicht dem schutzwürdigen Interesse des Betroffenen entgegensteht (Nr. 2) oder die Daten allgemein zugänglich sind (Nr. 3).

6.2.2.2.1 Das rechtsgeschäftliche oder rechtsgeschäftsähnliche Schuldverhältnis

Nach § 28 Abs. 1 S. 1 Nr. 1 BDSG kann eine Übermittlung und Speicherung personenbezogener Daten zu eigenen Geschäftszwecken zulässig sein, wenn dies für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses zwischen Google und dem Betroffenen erforderlich ist. An dieser Stelle ist der Begriff des Betroffenen abzugrenzen. Es ist zu unterscheiden, inwiefern sich die von Google verarbeiteten Daten ausschließlich auf den Glass-Träger als Betroffenen oder auf einen betroffenen Dritten beziehen.

Ein rechtsgeschäftliches Schuldverhältnis zwischen Google und dem Glass-Träger liegt aufgrund des Kaufvertrags über die Datenbrille vor.

[412] Art. 29-Datenschutzgruppe, WP 179, S. 23.

Danach könnte der Datenumgang von Google i. S. v. § 28 Abs. 1 S. 1 Nr. 1 BDSG zulässig sein. Wie in Kap. 6.1.2 festgestellt, handelt es sich bei den vom Glass-Träger erfassten Daten um Inhaltsdaten, die im Gegensatz zu Bestands- und Nutzungsdaten nicht für die Begründung und Durchführung eines Schuldverhältnisses i. S. d. TMG erforderlich sind. Allerdings setzt § 28 Abs. 1 S. 1 Nr. 1 BDSG nicht zwingend die Erforderlichkeit des Dateninhalts bzw. der Daten an sich für die Erfüllung des Schuldverhältnisses voraus, sondern verlangt eine Erforderlichkeit hinsichtlich der Erhebung, Verarbeitung und Nutzung. Demgemäß könnte sich die Zulässigkeit aus der Erforderlichkeit der Übermittlung und Speicherung ergeben.[413] Ohne diese Verarbeitung der Inhaltsdaten, ist die umfängliche Entfaltung von Google Glass und damit die Erfüllung des Vertragsverhältnisses zwischen dem Glass-Träger und Google Glass nicht möglich.[414] Aus diesem Grund ist die Übermittlung und Speicherung der von Google Glass erfassten Daten zur Erfüllung des Schuldverhältnisses erforderlich und der Datenumgang durch Google i. S. v. § 28 Abs. 1 S. 1 Nr. 1 BDSG grundsätzlich zulässig, soweit ausschließlich Daten des Glass-Trägers, als einzigem Betroffenen, verarbeitet werden.

Im Gegensatz dazu liegt bei dem Umgang mit Daten betroffener Dritte kein Schuldverhältnis zwischen dem Unternehmen und den Betroffenen vor. Folglich ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten betroffener Dritter durch Google mangels Schuldverhältnisses gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG unzulässig.[415]

6.2.2.2.2 Wahrung berechtigter Interessen

Die Übermittlung und Speicherung personenbezogener Daten durch Google könnte zur Wahrung berechtigter Interessen von Google gem.

---

413 Anders § 14 Abs. 1 TMG; *Kroschwald*, informationelle Selbstbestimmung in der Cloud, S. 204.

414 Kap. 2.2.

415 Vgl. Cloud Computing *Kroschwald*, Informationelle Selbstbestimmung in der Cloud, S. 206 f.

§ 28 Abs. 1 S. 1 Nr. 2 BDSG zulässig sein. Soweit Google Daten des Glass-Trägers i. S. v. § 28 Abs. 1 S. 1 Nr. 1 BDSG verarbeitet, tritt Nr. 2 hinter diesen Zulässigkeitstatbestand zurück.[416]

Die Beurteilung der Zulässigkeit der Verarbeitung personenbezogener Daten Dritter richtet sich schließlich nach § 28 Abs. 1 S. 1 Nr. 2 BDSG. Das berechtigte Interesse von Google an der Verarbeitung der Daten des Betroffenen könnte z. B. in der ordnungsgemäßen Dienstbereitstellung und -erbringung liegen, sodass auch von einer Erforderlichkeit des Datenumgangs zur ordnungsgemäßen Diensterbringung ausgegangen werden könnte. Jedoch kann dies nur ein berechtigtes Interesse sein, wenn die Daten rechtmäßig erworben wurden.[417] Infolgedessen könnten unter Berücksichtigung der Ergebnisse des Kap. 6.2.1 lediglich bei besonderen Einzelfällen die Daten auf Grundlage von § 28 Abs. 1 S. 1 Nr. 2 BDSG von Google verarbeitet werden.

Ist von einer Erforderlichkeit des Datenumgangs zur Wahrung berechtigter Interessen seitens Google auszugehen, müssen diese wiederum mit möglichen bestehenden schutzwürdigen Interessen des Betroffenen abgewogen werden. Dabei muss berücksichtigt werden, dass vom Glass-Träger Daten jeglicher Art, insbesondere sensitive Daten sowie Daten besonders schutzwürdiger Betroffener auf den Google-Servern gespeichert werden können. Zudem könnten auch solche Daten vorliegen, die der einzelne Glass-Träger erst gar nicht hätte erfassen dürfen.[418] Sind die bereits erhobenen Daten mit den schutzwürdigen Interessen des Betroffenen als nicht vereinbar zu bewerten, ist dies auch bei der Beurteilung des Datenumgangs von Google zu beachten.[419] Zugunsten des Betroffenen ist anzuführen, dass dieser meist keine Kenntnis über Art und Umfang der Inanspruchnahme von Google hat. Unter Berücksichtigung dieser Umstände kann davon ausgegangen

---

416 *Wedde*, in: Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 14; *Simitis*, in: Simitis, § 28 BDSG, Rn. 54.

417 *Hoeren*, in: Roßnagel, Hdb DS, 4.6, Rn. 32; *Bergmann/Möhrle/Herb*, § 28 BDSG, Rn. 233.

418 Siehe *Kroschwald*, Informationelle Selbstbestimmung in der Cloud, S. 226.

419 Vgl. 6.2.1.

werden, dass die schutzwürdigen Interessen des Betroffenen einer Übermittlung und Speicherung durch Google grundsätzlich entgegenstehen und somit der Datenumgang durch Google als unzulässig gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG zu bewerten ist.

6.2.2.2.3 Allgemein zugängliche Daten

Der Datenumgang durch Google könnte nach § 28 Abs. 1 S. 1 Nr. 3 BDSG zulässig sein, soweit es sich um allgemein zugängliche Daten handelt und schutzwürdige Interessen der Betroffenen nicht offensichtlich überwiegen. Unter Berücksichtigung der Ausführungen in Kapitel 6.2.1.2.3 ist davon auszugehen, dass die Daten, die übermittelt und gespeichert werden, nicht allgemein zugänglich i. S. v. § 28 Abs. 1 S. 1 Nr. 3 BDSG sind, sodass dieser ebenfalls als Erlaubnisnorm für den Datenumgang durch Google ausscheidet.

6.2.2.3 Rechtfertigung durch §§ 4b, 4c BDSG

Weiter könnte für die Übermittlung der personenbezogenen Daten an Google, mit Sitz im europäischen Ausland, die Erlaubnistatbestände der §§ 4b, 4c BDSG[420] heranzuziehen sein. § 4b BDSG stellt keine eigenständige Rechtsgrundlage für die Datenübermittlung ins Ausland dar.[421] Demnach ist auf der ersten Stufe zu prüfen, ob die Datenübermittlung nach den allgemeinen Grundsätzen des BDSG gem. § 4 Abs. 1 BDSG zulässig ist. In diesem Fall ist die Regelung des § 28 BDSG zur Beurteilung der ersten Stufe maßgebend. Liegt demnach eine Rechtmäßigkeit des Datenumgangs vor,[422] ist die Zulässigkeit auf der zweiten Stufe gem. §§ 4b und 4c BDSG zu prüfen.[423]

Gem. § 4b Abs. 2 S. 2 BDSG sind internationale Datenübermittlungen grundsätzlich verboten, wenn der Betroffene ein schutzwürdiges Inte-

420 Setzen Artt. 25, 26 DSRL um.
421 *v. d. Bussche*, in: Plath, § 4b BDSG, Rn. 4.
422 Kap. 6.2.2.2.1, 6.2.2.2.
423 *v. d. Bussche*, in: Plath, § 4b BDSG, Rn. 16; *Gola/Schomerus*, § 4b BDSG, Rn. 6; *Gabel*, in: Taeger/Gabel, § 4b BDSG, Rn. 18.

resse am Ausschluss der Übermittlung hat, insbesondere dann, wenn kein angemessenes Datenschutzniveau i. S. v. § 4b Abs. 3 BDSG beim Datenempfänger gewährleistet ist.[424] Google hat sich den Safe Harbor Principles der Federal Trade Commission unterstellt und sich verpflichtet, diese einzuhalten.[425] Bisher wurde die darin geregelte Selbstzertifizierung US-amerikanischer Unternehmen als Grundlage für Datenübermittlungen in die USA herangezogen. Allerdings hat der EuGH mit Urteil vom 6.10.2015 die Entscheidung der Europäischen Kommission vom 26.7.2000 (2000/520/EG) zur Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, für ungültig geklärt.[426] Danach ist eine Datenübermittlung auf Grundlage des Safe Harbor Abkommens seit Verkündung des Urteils nicht mehr zulässig. Aktuell wird über ein neues Safe Harbor Abkommen verhandelt, mit dessen Abschluss noch Anfang 2016 zu rechnen ist.[427] Allerdings ist diese Problematik nicht Gegenstand der Arbeit, weshalb auf die aktuelle Diskussion und auf entsprechende Literatur zu verweisen ist.[428]

6.2.2.4 Einwilligung als Legitimation

Ferner ist zu prüfen, ob der Datenumgang durch Google seine Legitimation durch die Einwilligung gem. §§ 4 Abs. 1, 4a BDSG erfahren könnte. Eine Einwilligung im Rahmen des Datenumgangs durch

---

424 Das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung und das Vorliegen eines angemessenen Datenschutzniveaus müssen getrennt geprüft werden. Schutzwürdige Interessen können sich bspw. aus der besonderen Sensibilität der zur Übermittlung vorgesehenen Daten ergeben; *Gola/Schomerus*, § 4b BDSG, Rn. 7; anders als die DSRL verlangt § 4b Abs. 2 S. 2 BDSG lediglich ein angemessenes Schutzniveau bei der empfangenden Stelle, kritisch dazu *Roßnagel/Jandt/Richter*, DuD 2014, 545 (547); *Simitis*, in: Simitis, § 4b BDSG, Rn. 73 ff.

425 U.S.-EU Safe Harbor List, Internetquelle.

426 EuGH, Urteil v. 6.10.2015 – C-362/14.

427 *Sokolov*, heise-online v. 7.1.2016, Internetquelle.

428 Siehe z.B. *Peintinger*, ZD-Aktuell 2016, 04172; *Weichert*, VuR 2016, 1; *Spies*, ZD-Aktuell 2015, 04869 m.w.N.; *Schröder*, ZD 2015, 501; *Roßnagel/Jandt/Richter*, DuD 2014, 545; *Schaar*, ZRP 2013, 214; *Räther/Seitz*, MMR 2002, 425; *Spies*, ZD 2013, 535; *Simitis*, in: Simitis, § 4b BDSG, Rn. 38 ff.

Google kommt als Erklärung des betroffenen Dritten gegenüber Google oder, soweit Daten des Glass-Trägers verwendet werden, auch des Glass-Trägers selbst gegenüber Google in Betracht. Die Einwilligung des Glass-Trägers in den Datenumgang tritt als Rechtsgrundlage zurück, soweit in diesem Fall § 28 Abs. 1 S. 1 Nr. 1 BDSG den Datenumgang erlaubt.[429] Hinsichtlich der Einwilligung betroffener Dritter ist es für Google als verantwortliche Stelle nahezu unmöglich zu ermitteln, wer Betroffener ist und von welchen Personen folglich eine Einwilligung vorliegen müsste.[430] Somit scheidet die Einwilligung als Legitimationsgrundlage für den Umgang mit personenbezogenen Daten Dritter durch Google aus.

6.2.2.5 Zwischenfazit

Beim Datenumgang durch Google ist nach der aktuellen Rechtsprechung deutsches Datenschutzrecht anwendbar, woraufhin § 28 BDSG als Erlaubnistatbestand im Vordergrund steht. Auf Grundlage des § 28 Abs. 1 S. 1 Nr. 1 BDSG können nur Daten, die sich sicher und ausschließlich auf den Glass-Träger beziehen von Google verarbeitet werden. Daten betroffener Dritter könnten nach § 28 Abs. 1 S. 1 Nr. 2 BDSG von Google verarbeitet werden, wobei dies angesichts entgegenstehender schutzwürdiger Interessen der Betroffen grundsätzlich als datenschutzrechtlich unzulässig zu bewerten ist. Die Einwilligung als Legitimation scheidet beim Datenumgang durch Google aus.

[429] *Gola/Schomerus*, § 4 BDSG, Rn. 15.
[430] Kap. 6.2.1.4.

7 Gestaltungsvorschläge

Die bisherigen Ausführungen zeigen, welche Gefahren neue technische Entwicklungen des Ubiquitous Computing bzw. Wearable Computing am Beispiel von Google Glass mit sich bringen können. Besonders im Hinblick darauf, dass § 28 Abs. 1 S. 1 Nr. 2 BDSG in den meisten Fällen den einschlägigen Erlaubnistatbestand im Rahmen von Google Glass darstellt, könnten die darin enthaltenen Generalklauseln des „berechtigten Interesses" und das Gebot zur Abwägung mit „schutzwürdigen Interessen" für Interessierte den Weg zu einer vielfältigen und umfassenden Datenverarbeitung für ihre Zwecke eröffnen.[431] Insofern wird angesichts der fortschreitenden technischen Entwicklung das bisherige datenschutzrechtliche Schutzprogramm in Frage gestellt, wobei gleichzeitig das Recht auf informationelle Selbstbestimmung in einer technisierten Welt verstärkt werden muss je größer die Risiken für die freie Entfaltung von Individuen durch eine Datenverarbeitung werden.[432] Demzufolge muss eine Anpassung und Fortentwicklung des datenschutzrechtlichen Schutzprogramms gefordert werden, um den wachsenden Risiken der zukünftigen I&K-Technologie entsprechend begegnen zu können.[433]

Im Fall von Google Glass ist zu überlegen, inwiefern dem daraus resultierenden rechtlichen Gefahrenpotenzial entsprechend begegnet werden kann.[434] Trotz der rechtlichen Risiken, die durch die Glass-Träger als vermeintliche „rücksichtslose Idioten"[435] ausgelöst werden und der Kritik der Bewegung „Stop the Cyborgs",[436] ist es vermutlich unvermeidbar, dass Datenbrillen wie Google Glass Teil des menschlichen Alltags werden. Aufgabe des Rechts muss es daher sein, die Inte-

---

431 Siehe zu dieser Problematik *Roßnagel/Müller*, CR 2004, 625 (630).
432 *Roßnagel/Müller*, CR 2004, 625 (628); *Roßnagel*, MMR 2005, 71 (75).
433 *Roßnagel/Müller*, CR 2004, 625 (628); *Roßnagel,* MMR 2005, 71; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts; *Friedewald/Lindner*, in: Mattern (Hrsg.), Informatisierung des Alltags, S. 207 (223).
434 Zum rechtlichen Gefahrenpotenzial siehe Kap. 4.
435 So *Weichert*, DANA 2/2013, 53 (55).
436 Stop the Cyborgs, Internetquelle.

ressen und Werte der Gesellschaft zu schützen, die trotz der dynamischen Technikentwicklung nicht aufs Spiel gesetzt werden dürfen.[437] In diesem Zusammenhang stößt das geltende Datenschutzrecht mit seinen normativ abgesicherten Verhaltensvorgaben an seine Grenzen.[438] Daher ist das Recht vielmehr auf rechtsgemäße Technik angewiesen.[439] Unbedingt notwendig ist, dass Recht und Technik eine Allianz zum Schutz der informationellen Selbstbestimmung eingehen müssen.[440]

Im Folgenden werden Gestaltungsvorschläge i. S. d. Privacy by Design für Google Glass vorgestellt, die das rechtliche Gefahrenpotenzial mindern und die schutzwürdigen Interessen der Betroffenen berücksichtigen könnten. Die Vorschläge orientieren sich an den datenschutzrechtlichen Prinzipien, die das grundsätzliche Schutzprogramm im Datenschutzrecht darstellen.[441]

7.1 Privacy by Design

Privacy by Design bzw. Datenschutz durch Technik soll die Datenschutzanforderungen schon bei der Entwicklung und beim Einsatz von IT-Systemen und Anwendungen berücksichtigen.[442] Danach soll die I&K-Technologie selbst als Instrument zur Erreichung der rechtlichen Ziele und Schutzaufträge dienen.[443] Google, als Hersteller und Entwickler, ist Adressat dieses Konzeptes und daran gehalten, durch frühzeitige Integration datenschutzfördernder Techniken (Privacy En-

---

437 *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung, S. 11 ff.

438 Zur Kritik am gegenwärtigen Datenschutzkonzept bereits umfassend *Roßnagel/Pfitzmann/Garstka*, Modernisierung des allgemeinen Datenschutzrechts.

439 *Roßnagel*, in: Klumpp/Kubicek/Roßnagel (Hrsg.), Next Generation Information Society?, S. 423 (430).

440 *Simitis*, DuD 2000, 714 (725); *Roßnagel*, in: Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik S. 17 (23 ff.); *v. Stechow*, Datenschutz durch Technik, S. 60.

441 Ausführlich zu den Datenschutzprinzipien *Trute*, in: Roßnagel, 2.5, Rn. 32 ff.; *Tinnefeld/Buchner/Petri,* Einführung in das Datenschutzrecht, S. 237 ff.

442 *Rost/Bock*, DuD 2011, 30 ff.

443 *Niemann/Scholz*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, S. 109 (113 f.); *Roßnagel*, in: Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik?, S. 17 (23); *Dix*, in: Roßnagel, Hdb DS, 3.5., m.w.N.

hancing Technologies)[444] in Google Glass präventiv potenzielle rechtliche Risiken zu vermeiden.[445] Denn was technisch verhindert wird oder technisch nicht möglich ist, muss nicht mehr verboten und überwacht werden.[446] Hinzu kommt der Aspekt des Privacy by Default bzw. Datenschutz durch Standardeinstellungen. Demnach hat Google bereits auf der Grundlage von Standardeinstellungen die erforderliche Datennutzung auf ein Mindestmaß zu beschränken.[447] Diesem Konzept könnte bereits dadurch Rechnung getragen werden, dass sich der Glass-Träger selbst manuell mit dem Internet verbinden muss und dies nicht mehr automatisch erfolgt.

Des Weiteren könnte zum Konzept des Privacy by Design § 9 BDSG hinzugezogen werden. Diese Norm verlangt von den datenverarbeitenden Stellen, die Anforderungen des BDSG durch die erforderlichen technischen und organisatorischen Maßnahmen umzusetzen.[448] Infolgedessen müsste Google unter Berücksichtigung des Schutzziels des BDSG Google Glass bzw. die Kombination aus Hardware, Software, Daten und organisatorischen Maßnahmen datenschutzgerecht realisieren, um einen gesetzeskonformen Dienst anbieten zu können.[449] Ein eminenter Vorteil ergäbe sich auch dadurch, dass die eingebaute Technik dann unabhängig von nationalen Grenzen wirksam wäre und somit auch in anderen Ländern, in denen das Persönlichkeitsrecht des einzelnen weniger gut geschützt ist, seine Wirkung entfalten könnte.[450]

---

444 Zu Privacy Enhancing Technology vgl. *Borking*, DuD 2001, 607 ff.; *Hansen*, in: Roßnagel, Hdb DS, 3.3 m. w. N.

445 Vgl. *Niemann/Scholz*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, S. 109 (113 f.); *Hornung*, ZD 2011, 51.

446 *Roßnagel*, in: Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik?, S. 17 (23).

447 *Niemann/Scholz*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, S. 109 (114 f.); *Roßna gel*, in: Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik?, S. 17 (24).

448 Ausführlich zu § 9 BDSG v. *Stechow,* Datenschutz durch Technik, S. 73 ff.; *Ernestus*, in: Simitis, § 9 BDSG.

449 *Hansen*, in: Roßnagel, Hdb DS, 3.3, Rn. 25.

450 *v. Stechow*, Datenschutz durch Technik, S. 61 m.w.N.

7.1.1 Förderung der Transparenz beim Erfassungsvorgang

Durch die unbemerkte und unberechenbare Erfassung von personenbezogenen Daten Dritter durch Google Glass ist es kaum möglich zu wissen „wer was wann und bei welcher Gelegenheit über sie weiß".[451] Dadurch wird der in § 4 Abs. 2 S. 1 BDSG normierte Direkterhebungsgrundsatz verletzt, wonach Daten grundsätzlich beim Betroffenen zu erheben sind. Zum Schutz des Rechts auf informationelle Selbstbestimmung soll dieser Grundsatz den Betroffenen die Möglichkeit eröffnen, über die Tatsache der Erhebung und die erhebende Stelle Kenntnis zu erlangen und entsprechend handeln zu können.[452] Dazu nennt das BVerfG zur Herstellung von Transparenz die Instrumente der Aufklärung, Auskunft und Löschung.[453] Gleichzeitig wird durch die Datentransparenz auch die Möglichkeit für erfolgreichen Selbstdatenschutz[454] geschaffen, denn ohne über die Gefahren für das Recht auf informationelle Selbstbestimmung informiert zu sein, können Betroffene in den meisten Fällen auch nicht auf diese reagieren.[455]

Um die geforderte Transparenz bei der Datenerhebung im Rahmen von Google Glass herzustellen ist an die Kamera bzw. der Kamerafunktion der Datenbrille anzuknüpfen. Die Transparenz könnte durch deutliche Hinweise auf die Datenerhebung und -verarbeitung verbessert werden. Es müsste auch ohne sichtbares Anvisieren von außen erkennbar sein, wenn Kameraaufnahmen gemacht werden. Die intransparente Datenerhebung könnte dadurch verhindert werden, wenn beim Aktivieren der Kamerafunktion ein deutliches von Dritten erkennbares Aufnahmesignal sichtbar wird, anstatt des einmaligen kurzen Aufleuchtens des Prismas. Vergleichbar mit der in § 6b Abs. 2 BDSG geforderten Kenntlichmachung müsste das Leuchtsignal für die gesamte Dauer der Kameraaufnahme in einer gut er-

451 BVerfGE 65, 1 (43); siehe Kap. 4.1.
452 *Scholz/Sokol*, in: Simitis, § 4 BDSG, Rn. 20.
453 BVerfGE 65, 1 (46).
454 Zum Konzept des Selbstdatenschutzes *Roßnagel*, in: Roßnagel, Hdb DS, 3.4.
455 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 82, 90.

kennbaren Farbe neben dem Prisma aufleuchten.[456] Zudem könnte anhand der Farbe des Leuchtsignals noch zwischen einer Foto- und Videoaufnahme unterschieden werden. Dadurch wäre zumindest für Betroffene aus der Nähe erkennbar, wann eine Aufnahme durch einen Glass-Träger erfolgt. Würden allerdings aus der Ferne Kameraaufnahmen angefertigt, wäre das Leuchtsignal für betroffene Personen allerdings nur schwer oder nicht erkennbar.

Ebenfalls würde es zu einer entspannten Atmosphäre in der Öffentlichkeit führen, wenn die Glass-Träger ihre Kamera mit einem blickdichten Deckel abdecken würden.[457] Dadurch werden ein möglicher Überwachungsdruck und ein Unwohlsein der Personen vermieden, wenn sie anhand des Deckels erkennen, dass der Glass-Träger von seiner Kamera keinen Gebrauch machen kann und somit keine personenbezogenen Daten Dritter erhoben werden können. Eine solche Vorrichtung verhindert zwar eine bildliche Aufnahme jedoch keinesfalls eine Tonaufnahme. Dennoch könnte das gleiche Ziel erreicht werden, wenn die Tonaufnahme nur zusammen mit der Kamera funktionieren würde. An dieser Stelle müsste Google eine softwaretechnische Lösung finden, um mit dem Aufsetzen des Deckels die Möglichkeit einer Datenerhebung durch Bild- und Tonaufnahmen auszuschließen.

7.1.2 Datenvermeidung und Datensparsamkeit

Durch Google Glass ist es möglich eine große Masse an Daten mit unterschiedlichster Qualität zu erheben und zu sammeln. Aus diesem Grund muss der Grundsatz der Datenvermeidung und Datensparsamkeit gem. § 3a BDSG in den Vordergrund gerückt werden. Danach dürfen so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden sowie nach Möglichkeit die Techniken der Anonymisierung und Pseudonymisierung berücksichtigt werden.

---

456 Vgl. *Roßnagel*, MMR 2005, 71 (73); *Henning/Richter*, KommunalPraxis Wahlen 2014, 9 ff.

457 Siehe *Henning/Richter*, KommunalPraxis Wahlen 2014, 9 ff.

Aufgrund der momentan noch mangelnden Transparenz beim Erfassungsvorgang ist der Betroffene nicht in der Lage, die vielfältigen Datenverarbeitungen zu erkennen oder zu kontrollieren, sodass Datenschutz gewährleistet werden muss, indem der Personenbezug von Daten von Anfang an vermieden oder auf das absolut notwendige Maß begrenzt werden muss.[458] Im Rahmen der Weiterentwicklung und technischen Gestaltung von Google Glass müssen deshalb eine datensparsame Systemgestaltung in den Fokus der Forderungen geraten sowie Möglichkeiten sinnvoller anonymer und pseudonymer Anwendungen bedacht werden.[459]

Neben Standardeinstellungen, die eine automatische Verbindung mit dem Internet unterbinden, könnte ähnlich wie bei der Videoüberwachung eine Art Privacy Filter eingesetzt werden. Die Gesichtserkennungstechnologie des Privacy Filters ermöglicht durch die Verschleierung der vom Videosystem erfassten Gesichter die Anonymisierung der dazugehörenden Personen.[460] Der Glass-Träger könnte den Privacy Filter einschalten, sofern er sich in der Öffentlichkeit bewegt und Aufnahmen von der Umgebung und sich dort aufhaltenden Personen machen möchte, ohne auf deren Identifizierung abzuzielen. Durch diese Software könnte das Ziel der Datenvermeidung und Datensparsamkeit des § 3a BDSG erreicht werden.

In diesem Zusammenhang ist Google jedoch verpflichtet, bereits i. R. d. Aufklärung der Glass-Träger tätig zu werden. Es ist zwar technisch bis zu einem gewissen Maß möglich die personenbezogene Datenerhebung und -verarbeitung zu beschränken, dennoch liegt es letztlich allein beim Glass-Träger selbst, welche Daten dieser mit der Datenbrille erfasst. Vorrangig ist daher, die bisherige Datenschutzerklärung von Google Glass an die gesellschaftlichen Interessen und den Schutz des Persönlichkeitsrechts anzupassen. Es könnte bereits mithil-

458 Vgl. *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 37; *Roßnagel*, MMR 2005, 71 (74).
459 *v. Stechow*, Datenschutz durch Technik, S. 83 f.
460 Siehe dazu *v. Stechow*, Datenschutz durch Technik, S. 53 ff.

fe der deutlich und klar formulierten Datenschutzerklärung möglich sein, die Glass-Träger in gewisser Weise zu sensibilisieren und dementsprechend die Persönlichkeitsrechte Dritter bei der Nutzung von Google Glass angemessen zu berücksichtigen.

7.1.3 Beschränkung der weiteren Nutzung der personenbezogenen Daten

Durch die zwingende Anbindung von Google Glass an die Google Infrastruktur liegt in den meisten Fällen ein Eingriff in das Recht auf informationelle Selbstbestimmung in verstärkter Form vor. Durch den Glass-Träger und durch Google wird das informationelle Selbstbestimmungsrecht des Betroffenen beeinträchtigt. Um diese enorme Beeinträchtigung zu vermeiden, wäre ein Vorschlag, Google seine Datenbrille losgelöst von der Google Infrastruktur anbieten zu lassen. Dies erfordert zunächst einen größeren internen Speicher der Google Glass selbst, sodass alle vom Glass-Träger erfassten Daten nur dort gespeichert werden können. Des Weiteren müsste Google die Software so gestalten, dass dem Nutzer die jeweiligen Anwendungen zur Verfügung gestellt werden, ohne vorher die dafür notwendigen Daten an unternehmenseigene Server zu übermitteln, zu speichern und wieder an Google Glass zurück übermitteln zu müssen.

Ferner muss im Hinblick auf Funktionen wie die Gesichtserkennung im Rahmen des Systemdatenschutzes reagiert werden.[461] Demnach darf Google Glass technisch nur das können, was auch erlaubt ist.[462] Google muss erkennen, Anwendungen, die das Persönlichkeitsrecht Betroffener gefährden soweit es möglich ist zu verhindern. Dies muss auf technischer Seite erfolgen sowie auch ein klares Votum dazu aus den „Terme of Use“ hervor gehen.[463]

---

461 Einzelheiten des Systemdatenschutzes *Dix*, in: Roßnagel, Hdb DS, 3.5.

462 *Roßnagel*, Datenschutz in einem informatisierten Alltag, S. 184.

463 Bisher verbietet Google in den Google Terms zwar die Gesichts- und Spracherkennung mit Glass, jedoch unter der Einschränkung, dass dies „derzeit“ gilt, Internetquelle.

7.2 Folgerung

Mit Wearable Computing Gadgets wie Google Glass werden neue Anwendungsprobleme für das geltende Datenschutzrecht geschaffen, die die bewährten Regulierungskonzepte in Frage stellen und die Entwicklung neuer Ansätze des Datenschutzrechts fordern.[464] Dennoch ist das geltende Datenschutzrecht als Rahmen für zukünftige Technologien zu berücksichtigen.[465] Im Hinblick auf die datenschutzrechtliche Bewertung ist zusammenfassend festzuhalten, dass Google Glass keine Herausforderung für das deutsche Recht darstellt, sondern vielmehr das Recht eine Herausforderung für Google Glass.[466] Folglich muss Google nach seinem Credo „Don't be evil",[467] nichts Schlechtes zu tun, im Hinblick auf die technischen Fähigkeiten und Entwicklungen unter Berücksichtigung der Anforderungen des Datenschutzrechts handeln. Werden die angeführten Vorschläge von Google berücksichtigt, führt dies in jedem Fall zu einer Minderung des Eingriffs in das informationelle Selbstbestimmungsrecht. Inwiefern diese Eingriffsminderung den Ausgang der datenschutzrechtlichen Zulässigkeitsprüfung insbesondere die Interessenabwägung im Einzelfall beeinflussen könnte, bleibt jedoch zu bezweifeln.

---

464 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts; *Roßnagel/Müller*, CR 2004, 625 (627).

465 Vgl. *Roßnagel/Jandt/Müller/Gutscher/Heesen*, Datenschutzfragen mobiler kontextbezogener Systeme, 57 ff.

466 So auch *Schwenke* in seinem Vortrag bei der Herbstakademie 2013, Internetquelle.

467 Google Philosophy, Internetquelle.

8 Fazit und Ausblick

Zusammenfassend kann festgehalten werden, dass eine Nutzung von Google Glass im Alltag, wie in dieser Arbeit geprüft, zwar in den Anwendungsbereich des BDSG fällt, jedoch aus datenschutzrechtlicher Sicht keine Legitimierung findet. Google Glass stellt trotz der technischen Neuerungen und Möglichkeiten keine Herausforderung für das deutsche Rechtssystem dar, da grundsätzlich das normative Schutzkonzept des BDSG greifen kann.[468] Vielmehr geht aus dem Ergebnis der datenschutzrechtlichen Bewertung hervor, dass Google Glass im derzeitigen Entwicklungsstadium noch großen Anpassungsbedarf hinsichtlich der Gefährdung des informationellen Selbstbestimmungsrechts benötigt.

Das Ergebnis der vorliegenden Arbeit wird u. a. durch den Umstand bestätigt, dass der ursprünglich angekündigte Markteintritt in Deutschland im Jahr 2014 verworfen wurde und Google im Januar 2015 bekannt gab, die Beta-Phase für Google Glass zu beenden und vorerst den Verkauf an Verbraucher einstellen. Das Unternehmen will das Programm Google Glass jedoch nicht aufgeben, sondern an der Entwicklung neuer Modelle arbeiten.[469] Grund für diese Reaktion könnte die Kritik aus Europa und die aktuelle Rechtsprechung des EuGH[470] sein, indem der Datenschutz in Europa hinsichtlich der Verantwortlichkeit erheblich gestärkt wurde. Danach ist es dem US-Unternehmen Google nicht mehr möglich, durch die Lokalisierung der Datenverarbeitung außerhalb der EU oder in vollzugsschwachen Mitgliedstaaten eine effektive Datenschutzkontrolle zu umgehen. Dies würde völlig andere Konsequenzen für Google als verantwortliche Stelle des Datenumgangs mit sich bringen. Unter Berücksichtigung der neuen Rechtslage und des aus Google Glass resultierenden rechtli-

468 *Solmecke/Kocatepe*, ZD 2014, 22 (26).
469 *Kramer*, heise-online v. 29.12.2015, Internetquelle; *dpa*, o. A., FAZ.NET v. 15.01.2015; *Wilkens*, heise-online v. 16.01.2015, Internetquelle.
470 EuGH, Urteil v. 13.05.2014 – C-131/12; EuGH, Urteil v. 6.10.2015 – C-362/14.

chen Gefahrenpotenzials, liegt es an Google i. S. d. Firmencredos „Don't be evil", seine Datenbrille entsprechend gesetzeskonform zu gestalten.

An diesem Umstand würde auch die Verabschiedung der Datenschutz-Grundverordnung (DS-GVO),[471] die einen einheitlichen Rechtsrahmen für den Datenschutz in der gesamten EU schaffen soll, nichts ändern. Die derzeit veröffentlichten Regelungen des Kompromissentwurfs würden ebenfalls zu keiner Änderung der datenschutzrechtlichen Beurteilung von Google Glass im Alltag führen.

Anhand der Ergebnisse dieser Ausarbeitung wird deutlich, welche Probleme Wearable Computing für das informationelle Selbstbestimmungsrecht schaffen könnte. Dennoch kann keine pauschale Bewertung getroffen werden, da jedes Wearable Computing Gadget auf seine Weise mehr oder weniger mit dem Datenschutzrecht in Berührung kommt. Im Hinblick auf künftige technische Innovationen im Bereich des Wearable Computing ist anzunehmen, dass es zum Schutz der informationellen Selbstbestimmung eines modifizierten und ergänzten Schutzprogramms bedarf, das den Konzepten und Instrumenten des Datenschutzes der Allgegenwärtigkeit der Datenverarbeitung angepasst wird.[472]

[471] Zum Kompromissentwurf über die Verordnung EU Nr. XXX/2016 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-GVO), Internetquelle.

[472] *Roßnagel/Jandt/Skistims/Zirfas*, Datenschutz bei Wearable Computing, S. 170.

Literatur

Arning, M./Moos, F./Schefzig, J., Vergiss (,) Europa! – Ein Kommentar zum EuGH, Urt. V. 13.5.2014 – RS. C-131/12 – Google/Mario Costeja Gonzalez, CR 2014, 460, CR 2014, 447-456.

Artikel 29-Datenschutzgruppe, WP 163, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 01189/09/DE, Brüssel 2009, http://www.cnpd.public.lu/de/publications/groupe-art29/wp163_de.pdf (Stand: 16.01.2015).

Artikel 29-Datenschutzgruppe, WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und Auftragsverarbeiter", 00264/10/DE, Brüssel 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf (Stand: 10.01.2015).

Artikel 29-Datenschutzgruppe, WP 179, Stellungnahme 8/2010 zum anwendbaren Recht, 0836-02/10/DE, Brüssel 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf (Stand: 16.01.2015).

Artikel 29-Datenschutzgruppe, WP 56, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU, 5035/01/DE/endg, Brüssel 2002, http://www.cnpd.public.lu/de/publications/groupe-art29/wp056_de.pdf (Stand: 16.01.2015).

Artikel 29-Datenschutzrgruppe, WP 192, Stellungnahme 2/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, 00727/12/DE, Brüssel 2012, http://www.cnpd.public.lu/de/publications/groupe-art29/wp192_de.pdf (Stand: 10.01.2015).

Bartelt, M., Datenschutz in sozialen Netzwerken – Eine datenschutzrechtliche Beurteilung im Lichte des deutschen und europäischen Rechts, Saarbrücken 2012 (zitiert: Bartelt, Datenschutz in sozialen Netzwerken).

Baumeler, C., Von kleidsamen Computern und unternehmerischen Universitäten – Eine ethnographische Organisationsstudie, Münster 2005.

Bäumler, H., Das TDDSG aus der Sicht eines Datenschutzbeauftragten, DuD 1999, 259-262.

Becker, M./Becker, F., Die neue Google-Datenschutzerklärung und das Nutzer-Metaprofil-Vereinbarung mit nationalen und gemeinschaftsrechtlichen Vorgaben, MMR 2012, 351-355.

Bendel, O., Die Datenbrille aus Sicht der Informationsethik – Problemanalysen und Lösungsvorschläge, Informatik-Spektrum, published online: 13.09.2014, DOI 10.1007/s00287-014-0836-y (zitiert: Bendel, Informatik-Spektrum Herbst 2014, 1 (4)).

Bergmann, L./Möhrle, R./Herb, A. (Hrsg.), Datenschutzrecht – Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und zum Bereichsspezifischen Datenschutz, 47. Ergänzungslieferung, München 2014.

Biermann, K./Pilath, M., US-Regierung zapft Facebook und Google an, Zeit-Online v. 07.06.2013, http://www.zeit.de/digital/datenschutz/2013-06/USA-Geheimdienste-Daten-Internet-Verizon (Stand: 28.11.2014).

Boeing, N./Stieler, W., Willkommen in der Matrix, Technology Review 10/2014, 26-32.

Borking, J., Privacy-Enhancing Technologies (PET) – Darf es ein Bitchen weniger sein?, DuD 2001, 607-615.

Brühann, U., Die Veröffentlichung personenbezogener Daten im Internet als Datenschutzproblem – Zur Rechtsprechung des Europäischen Gerichtshofs, DuD 2004, 201-209.

Brühann, U., Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG – Zugleich ein Beitrag zur Systematik von Richtlinien zur Rechtsangleichung im Binnenmarkt in der Rechtsprechung des Europäischen Gerichtshofs, EuZW 2009, 639-644.

Calliess, C./Ruffert, M. (Hrsg.), EUV/AEUV – Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 4. Auflage, München 2011.

Caspar, J., Geoinformationen und Datenschutz am Beispiel des Internetdienstes Google Street View, DÖV 2009, 965-974.

Glauß, U., Warum Googles Datenbrille an Produktbetrug grenzt, Die Welt v. 25.01.2015, http://www.welt.de/debatte/kommentare/article136740013/Warum-Googles-Datenbrille-an-Produktbetrug-grenzt.html (Stand: 26.01.2015).

Dammann, U., Internationaler Datenschutz, RDV 2002, 70-77.

Däubler, W., Gläserne Belegschaften? – Das Handbuch zum Arbeitnehmerdatenschutz, 5. Auflage, Frankfurt am Main 2010.

Däubler, W./Hjort, P./Schumert, M./Wolmerath, M. (Hrsg.), Arbeitsrecht – Individualarbeitsrecht mit kollektivrechtlichen Bezügen - Handkommentar, 3. Auflage, Baden Baden 2013.

Däubler, W./Klebe, T./Wedde, P./Weichert, T. (Hrsg.), Bundesdatenschutzgesetz – Kompaktkommentar zum BDSG, 4. Auflage, Frankfurt am Main 2014.

Dpa o. A., Google stoppt den Verkauf seiner Datenbrille, FAZ.NET v. 15.01.2015, http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google/google-glass-neuanfang-fuer-die-datenbrille-13372678.html (Stand: 16.01.2015).

Dpa o. A., Hessen weitet Einsatz von Schulterkameras für Polizisten aus, Focus-Online v. 01.10.2014, http://www.focus.de/regional/wiesbaden/polizei-hessen-weitet-einsatz-von-schulterkameras-fuer-polizisten-aus_id_4173371.html (Stand: 28.11.2014).

Dreier, H. (Hrsg.), Grundgesetz Kommentar Band 1, 3. Auflage, Tübingen 2013.

Dziemba, O./Wenzel, E., #Wir, Wie die Digitalisierung unseren Alltag verändert, 2014 München.

Ehlers, D. (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 3. Auflage, Berlin 2009 (zitiert: Bearbeiter, in: Ehlers).

Enzmann, M./Roßnagel, A., Realisierter Datenschutz für den Einkauf im Internet – Das Projekt DASIT, CR 2002, 141-150.

Epping, V. /Hillgruber, C. (Hrsg.), Grundgesetz Kommentar, 2. Auflage, München 2013.

Erd, R., Datenschutzrechtliche Probleme sozialer Netzwerke, NVwZ 2011, 19-22.

Erfurter Kommentar zum Arbeitsrecht, hrsg. v. *Müller-Glöge, R./Preis, U./Schmidt, I.*, 15. Auflage, München 2015 (zitiert: Bearbeiter in: ErfK).

Erfurth, R., Der neue Arbeitnehmerdatenschutz im BDSG, NJOZ 2009, 2914-2927.

Ernst, S., Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, 1917-1919.

Ernst, S., Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, 1917-1919.

Eßer, M./Kramer, P./v. Lewinski, K (Hrsg.), Auernhammer BDSG – Kommentar zum Bundesdatenschutzgesetz Nebengesetze, 4. Auflage, Köln 2014. (zitiert: Bearbeiter, in: Auernhammer).

Ferscha, A., Pervasive Computing: connected > aware > smart, in: Mattern, F. (Hrsg.), Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin Heidelberg 2007, S. 3-11 (zitiert: Bearbeiter, in: Mattern (Hrsg.), Informatisierung des Alltags).

Fitting,K. (Begr.)/Engels, G./Schmidt, I./Trebinger, Y./Linsenmaier, W. (Hrsg.), Betriebsverfassungsgesetz mit Wahlordnung – Handkommentar, 27. Auflage, München 2014 (zitiert: Fitting, § 75 BetrVG, Rn. 136 ff.).

Forgó, N./Krügel, T./Müllenbach, K., Zur datenschutz- und persönlichkeitsrechtlichen Zulässigkeit von Google Street View, CR 9/2010, 616-624.

Friedewald, M./Lindner, R., Datenschutz, Privatsphäre und Identität in intelligenten Umgebungen: Eine Szenarioanalyse, in: Mattern, F. (Hrsg.), Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin Heidelberg 2007, S. 207-233 (zitiert: Bearbeiter, in: Mattern (Hrsg.), Informatisierung des Alltags).

Frowein, J./Peukert, W. (Hrsg.), Europäische Menschenrechtskonvention – Kommentar, 2. Auflage, Stuttgart 1996.

Gierschmann, S./Saeugling, M. (Hrsg.), Systematischer Praxiskommentar Datenschutzrecht – Datenschutz aus Unternehmenssicht, Köln 2014.

Gola, P., Datenschutz am Arbeitsplatz –Handlungshilfen beim Einsatz von Intranet und Internet, E-Mail und Telefon, Video- und Ortungstechnik, 4. Auflage, Heidelberg 2012.

Gola, P., Die Entwicklung des Datenschutzrechts in den Jahren 1999/2000, NJW 2000, 3749-3757.

Gola, P./Klug, C., Grundzüge des Datenschutzrechts, München 2003.

Gola, P./Schomerus, R. (Hrsg.), BDSG – Bundesdatenschutz – Kommentar, 11. Auflage, München 2012.

Grabenwarter, C., Europäische Menschenrechtskonvention, 4. Auflage, München 2009 (zitiert: Grabenwarter, EMRK, § 22, Rn.).

Grabitz, E. (Begr.)/Hilf, M./Nettesheim, M. (Hrsg.), Das Recht der Europäischen Union, München 2009 (zitiert: Bearbeiter, in: Grabitz/Hilf).

Hansmann, U./Merk, L./Nicklous, M.S./Stober, T., Pervasive Computing Handbook, Berlin Heidelberg 2001.

Hardt, M., Googles wundertätige Datenbrille, FAZ.net v. 10.04.2014, http://www.faz.net/aktuell/feuilleton/einsatz-im-krankenhaus-googles-wundertaetige-datenbrille-12889891.html (Stand: 28.11.2014).

Henning, M., Richter, P., Der gefilmte Stimmzettel – Smartphones und Smartglasses in der Wahlkabine?, KommunalPraxis Wahlen 2014, 9-13.

Hornung, G., Datenschutz durch Technik in Europa – Die Reform der Richtlinie als Chance für ein modernes Datenschutzrecht, ZD 2011, 51-56.

Hornung, G., Die digitale Identität – Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden Baden 2005.

Hufen, F., Staatsrecht II Grundrechte, 3. Auflage, München 2011.

Jahn, D./Striezel, J., Google Street View is watching you, K&R 2009, 753-758.

Jandt, S./Roßnagel, A., Datenschutz in Social Networks, ZD 2011, 160-166.

Jandt, S./Roßnagel, A., Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?, MMR 2011, 637-642.

Janisch, W./Prantl, H., „Vertrauen in digitale Kommunikation ist beeinträchtigt", Süddeutsche.de v. 06.07.2013, http://www.sueddeutsche.de/politik/justizministerin-leutheusser-schnarrenberger-vertrauen-in-digitale-kommunikation-ist-beeintraechtigt-1.1714126 (Stand: 28.11.2014).

Janssen, J-K., Blinzel Brille, Google Glass: Neue Hardware, neue Software, c't 2014/6, 74.

Janssen, J-K., Warum Glass (noch) nicht funktioniert – Ernüchternde Langzeiterfahrungen mit Google Glass, c't 5/2013, 76-77.

Jarass, H. (Hrsg.), Charta der Grundrechte der Europäischen Union – unter Einbeziehung der vom EuGH entwickelten Grundrechte, der Grundrechtsregelungen der Verträge und der EMRK – Kommentar, 2. Auflage, München 2013 (zitiert: Jarass, Art. 7/51 GRC).

Jotzo, F., Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. Bei grenzüber-schreitendem Datenverkehr?, MMR 2009, 232-237.

Karg, M., Anmerkung zu einer Entscheidung des EuGH (Urteil v. 13.05.2014 – C- 131/12, ZD 2014, 350) zum Löschungsanspruch gegen Suchmaschinenbetreiber, ZD 2014, 359-361.

Karg, M., Anwendbares Datenschutzrecht bei Internet-Diensteanbietern – TMG und BDSG vs. Konzernstrukturen?, ZD 2013, 371-375.

Karg, M., Biometrische Verfahren zur Gesichtserkennung und Datenschutz in Sozialen Netzwerken, HFR 7/2012, 120-134.

Kartal-Aydemir, A./Krieg, R., Haftung von Anbietern kollaborativer Internetplattformen – Störerhaftung für User Generated Content?, MMR 2012, 647-652.

Kilian, W./Heussen, B. (Hrsg.), Computerrechts-Handbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, München 2008.

Kirchhof, F., Grundrechtsschutz durch europäische und nationale Gerichte, NJW 2011, 3681-3686.

Klas, B., Grenzen der Erhebung und Speicherung allgemein zugänglicher Daten, Edewecht 2012.

Klug, T., Prozessunterstützung für den Entwurf von Wearable-Computing-Systemen, Darmstadt 2008.

Kremp, M., Datenbrille im Test: Der Kitzel von Google Glass, Spiegel Online v. 07.06.2013, http://www.spiegel.de/netzwelt/gadgets/angefasst-google-Glass-im-test-a-904064.html (Stand: 27.11.2014).

Kremp, M., Neuheiten von Samsung, Garmin, Jawbone: Was taugen diese Fitness-Armbänder?, Spiegel Online v. 26.04.2014, http://www.spiegel.de/netzwelt/gadgets/fitness-armbaender-von-samsung-garmin-und-jawbone-a-965687.html (Stand: 22.11.2014).

Kroschwald, S., Informationelle Selbstbestimmung in der Cloud – Datenschutzrechtliche Bewertung und Gestaltung des Cloud Computing aus dem Blickwinkel des Mittelstands, Wiesbaden 2016.

Kroschwald, S., Kollektive Verantwortung für den Datenschutz in der Cloud, ZD 2013, 388-394.

Kühling, J./Seidel, C./Sivridis, A., Datenschutzrecht, 2. Auflage, Heidelberg 2011.

Lachenmann, M./Schwiering, S., Betrieb von Videokameras in PKW Datenschutzrechtliche (Un-)Zulässigkeit des Betriebs von On-Board-Kameras in Pkws, NZV 2014, 291-298.

Lindner, C., Persönlichkeitsrecht und Geo-Dienste im Internet – z. B. Google Street View/Google Earth, ZUM 2010, 292-301.

Linnhoff-Popien, C., Ubiquitous Computing – Machbarkeit und Grenzen, in: Eberspächer, J./v. Reden, W. (Hrsg.), Umhegt oder abhängig? – Der Mensch in einer digitalen Umgebung, Berlin Heidelberg 2006, S. 35-49 (zitiert: Bearbeiter, in: Eberspächer/Reden).

Llorente, R./Morant, M., Wearable Computers and Big Data: Interaction Paradigms for Knowledge Building in Higher Education, in, Peris-Ortiz, M./Garrigós-Simón, F./Pechuán, I. (Hrsg.), Innovation and Teaching Technologies – New Directions in Research, Practice and Policy, Heidelberg 2014, S. 127-139 (zitiert: Bearbeiter, in: Peris-Ortiz/Garrigós-Simon/Pechuán).

v. Mangoldt, H./Klein, F. (Begr.)/Starck, C. (Hrsg.), Kommentar zum Grundgesetz Band 1, 6. Auflage, München 2010.

Maschmann, F., Compliance versus Datenschutz, NZA-Beil. 2012, 50-58.

Mattern, F., Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen, in: Roßnagel, A./ Sommerlatte, T./Winand, U. (Hrsg.), Digitale Visionen, Zur Gestaltung allgegenwärtiger Informationstechnologien, Berlin 2008, S. 3-27 (zitiert: Bearbeiter, in: Roßnagel/Sommerlatte/Winand).

Mattern, F., Pervasive/Ubiquitous Computing, Informatik-Spektrum 2001, 145-147 (zitiert: Mattern, Informatik-Spektrum 2001).

Mattern, F., Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing, in: Mattern (Hrsg.), Total vernetzt, Szenarien einer informatisierten Welt, Berlin 2003, S. 1-38 (zitiert: Bearbeiter, in: Mattern (Hrsg.), Total vernetzt).

Maunz, T./Dürig, G. (Begr.)/Herzog, R./Herdegen, M./Scholz, R./Klein, H. (Hrsg.), Grundgesetz– Kommentar, 71. Ergänzungslieferung, München 2014 (zitiert: Bearbeiter, in: Maunz/Dürig).

Maurer, H., Der PC in zehn Jahren, Informatik Spektrum 27 (1) 2004, 44-50 (zitiert: Maurer, Informatik-Spektrum, 2004).

Meyer, J. (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage, Baden Baden 2014.

Meyer-Ladewig, J. (Hrsg.), Europäische Menschrechtskonvention – Handkommentar, 3. Auflage, Baden Baden 2011 (zitiert: Meyer-Ladewig, Art. 8 EMRK).

Miller, C., At Google, Bid to Put Its Glasses to Work, The New York Times v. 07.04.2014, http://www.nytimes.com/2014/04/08/technology/google-begins-a-push-to-take-glass-to-work.html?_r=2 (Stand: 27.11.2014).

Müller-Broich, J. (Hrsg.), Telemediengesetz, Baden Baden 2012.

Münch, I. (Begr.)/Kunig, P. (Hrsg.), Grundgesetz Kommentar, Band 1, 6. Auflage, München 2012.

Niemann,F./Scholz,P., Privacy by Design und Privacy by Default – Wege zu einem funktionierenden Datenschutz in Sozialen Netzwerken, in: Peters, F./Kersten, H./Wolfenstetter, K., (Hrsg.) Innovativer Datenschutz, Berlin 2012, S. 109-145 (zitiert: Bearbeiter, in: Peters/Kersten/Wolfenstetter, Innovativer Datenschutz).

Oppermann, T./Classen, C./Nettesheim, M, Europarecht – Ein Studienbuch, 6. Auflage, München 2014.

Pauly, D./Ritzer, C./Geppert, N., Gilt europäisches Datenschutzrecht auch für Niederlassungen ohne Datenverarbeitung? – Weitreichende Folgen für internationale Konzerne, ZD 2013, 423-426.

Paletta, G., „Stört nicht beim Schießen": Polizei testet Google Glass, ZDF Online v. 08.02.2014, http://blog.zdf.de/hyperland/2014/02/google-glass-und-die-polizei (Stand: 28.11.2014).

Peintinger, S., Aktueller Zwischenstand zu Safe Harbor, ZD-aktuell 2016, 04172.

Pfaff, D./Skiera, B., Ubiquitous Computing – Abgrenzung, Merkmale und Auswirkungen aus betriebswirtschaftlicher Sicht, in: Britzelmaier, B./Geberl, S./Weinmann, S. (Hrsg.), Der Mensch im Netz – Ubiquitous Computing, 4. Liechtensteinisches Wirtschaftsinformatik-Symposium an der FH Liechteinstein, Stuttgart 2002, S. 25-39 (zitiert: Bearbeiter, in: Britzelmaier/Geberl/Weinmann, Der Mensch im Netz).

Plath, K. (Hrsg.), BDSG – Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG, Köln 2013.

Polenz, S., Die Datenverarbeitung durch und via Facebook auf dem Prüfstand, VuR 2012, 207-2013.

Porteck, S./Sokolov, D./Zota, V., Glass durchschaut, Googles Datenbrille im Test: Nerd-Spielzeug oder mobile Zukunft?, c't 2013/13, 62-71.

Räther, P./Seitz, N., Übermittlung personenbezogener Daten in Drittstaaten - Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, 425-433.

Richardi, R (Hrsg.), Betriebsverfassungsgesetz mit Wahlordnung – Kommentar, 14. Auflage, München 2014.

Richardi, R./Dörner, H./Weber, C. (Hrsg.), Personalvertretungsrecht – Bundespersonalvertretungsgesetz mit Erläuterungen zu den Personalvertretungsgesetzen der Länder – Kommentar, 4. Auflage, München 2012.

Roßnagel, A./Jandt, S./Richter, P., Die Zulässigkeit der Übertragung personenbezogener Daten in die USA im Kontext der NSA-Überwachung, DuD 2014, 545-551.

Roßnagel, A. (Hrsg.), Beck'scher Kommentar zum Recht der Telemediendienste – Telemediengesetz, Jugendmedienschutz-Staatsvertrag (Auszug), Signaturgesetz, Signaturverordnung, Vorschriften zum elektronischen Rechts- und Geschäftsverkehr, München 2013 (zitiert: Bearbeiter, in: Roßnagel).

Roßnagel, A. (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2013 (zitiert: Bearbeiter, in: Roßnagel, Hdb DS).

Roßnagel, A./Jandt, S./Skistims, H./Zirfas, J., Datenschutz bei Wearable Computing – Eine juristische Analyse am Beispiel von Schutzanzügen, Wiesbaden 2012 (zitiert: Roßnagel/Jandt/Skistims/Zirfas, Datenschutz bei Wearable Computing).

Roßnagel, A./Schnabel, C., Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534-3538.

Roßnagel, A., Datenschutz in einem informatisierten Alltag – Gutachten, 2007 Berlin.

Roßnagel, A., Informationelle Selbstbestimmung in der Welt des Ubiquitous Computing, in: Mattern, F. (Hrsg.), Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin Heidelberg 2007, S. 265-291 (zitiert: Bearbeiter, in: Mattern (Hrsg.), Informatisierung des Alltags).

Roßnagel, A., Jandt, S., Müller, J., Gutscher, A., Heesen, J., Datenschutzfragen mobiler kontextbezogener Systeme, 2006 Wiesbaden.

Roßnagel, A., Modernisierung des Datenschutzrechts in einer Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71-75.

Roßnagel, A., Datenschutz 2015 – in einer Welt des Ubiquitous Computing, in: Bizer, J./v. Mutius, A./Petri, T./Weichert, T. (Hrsg.), Innovativer Datenschutz 1992-2004 – Wünsche, Wege, Wirklichkeit, Für Helmut Bäumler, Kiel 2004, S. 335-351.

Roßnagel, A./Müller, J., Ubiquitous Computing – neue Herausforderung für den Datenschutz – Ein Paradigmenwechsel und die von ihm betroffenen normativen Ansätze, CR 2004, 625-632.

Roßnagel, A., Recht und Technik in der globalen Informationsgesellschaft, in: Klumpp, D./Kubicek, H./Roßnagel, A. (Hrsg.), Next generation information society? – Notwendigkeit einer Neuorientiertung, Mössingen-Talheim 2003, S. 423-433.

Roßnagel, A., Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz, Baden-Baden 2001 (zitiert: Bearbeiter, in: Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik?).

Roßnagel, A./Pfitzmann, A./Garstka, H., Modernisierung des Datenschutzrechts – Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.

Roßnagel, A., Rechtswissenschaftliche Technikfolgenforschung – Umrisse einer Forschungsdisziplin, Baden Baden 1993.

Schaar, P., Lässt sich die globale Internetüberwachung noch bändigen?, ZRP 2013, 214-216.

Schaffland, H.-J./Wiltfang, N. (Hrsg.), Bundesdatenschutzgesetz – BDSG – Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Ergänzungslieferung 4/13, Berlin 2013.

Schapiro, L., Die neuen Musiktauschbörsen unter „Freunden", ZUM 2008, 273-282.

Scheja, G., Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank – Eine Untersuchung unter besonderer Berücksichtigung der §§ 4b, 4c BDSG, Baden Baden 2006.

Schenk, M./Niemann, J./Reinmann, G./Roßnagel, A. (Hrsg.), Digitale Privatsphäre – Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen, 2012 Berlin.

Schmidt, A., Eingebettete Interaktion – Symbiose von Mensch und Information, in: Mattern, F. (Hrsg.), Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin Heidelberg 2007, S. 77-103 (zitiert: Bearbeiter, in: Mattern (Hrsg.), Informatisierung des Alltags).

Schmidt, B., Beschäftigtendatenschutz in § 32 BDSG, DuD 2010, 207-210.

Schmidt-Bleibtreu, B./Klein, F. (Begr.)/Hofmann, H./Hopfauf, A. (Hrsg.), Kommentar zum Grundgesetz, 12. Auflage, Köln 2011.

Schnabel, C., Das Recht am eigenen Bild und der Datenschutz, ZUM 2008, 657-662.

Schröder, C., Safe Harbor: Ein Ende mit Schrecken – Wann kommt Safe Harbor 2.0?, ZD 2015, 501-502.

Schwarze, J. (Hrsg.)/Becker, U./Hatje, A./Schoo, J., EU-Kommentar, 3. Auflage Baden Baden 2012.

Schweizer, R., Die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zum Persönlichkeits- und Datenschutz, DuD 2009, 462-468.

Schwenke, T., Google Glass – Eine Herausforderung für das Recht, K&R 11/2013, 685-691.

Schwenke, T., Google Glass – Herausforderung für das Recht, in: Taeger, J. (Hrsg.), Tagungsband Herbstakademie 2013 – Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter, Oldenburg 2013, S. 215-235.

Selig, R., Arbeitnehmerdatenschutz – Das Datenschutzrecht im Spannungsverhältnis von Mitarbeiterkontrolle und Arbeitnehmerinteressen, Berlin 2011.

Simitis, S. (Hrsg.), Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden 2014.

Simitis, S., Auf dem Weg zu einem neuen Datenschutzkonzept – Die zweite Novellierungsstufe des BDSG, DuD 2000, 714-726.

Solmecke, C., Kocatepe, S., Google Glass – Der Gläserne Mensch 2.0, ZD 1/2014, 22-27.

Solmecke, C., Vondrlik, S., Rechtliche Probleme bei Produkten mit serverbasierten Zusatzdiensten, Was passiert, „wenn der Kühlschrank keine Einkaufsliste mehr schreibt…", MMR 2013, 755-760.

Sörup, T., Anmerkung zum Urteil des EuGH Löschungsanspruch gegen Google – „Recht auf Vergessen", MMR 2014, 455-465.

Spies, A., Keine „Genehmigungen" mehr zum USA-Datenexport nach Safe Harbor?, ZD 2013, 535-538.

Spies, A., Anmerkungen zum Positionspapier der deutschen Datenschutzbeauftragten zu Safe Harbor, ZD-Aktuell 2015, 04869.

Spindler, G./Schuster, F. (Hrsg.), Recht der elektronischen Medien, 2. Auflage, München 2011.

v. Stechow, C., Datenschutz durch Technik – Rechtliche Förderungsmöglichkeiten von Privacy Enhancing Technologies am Beispiel der Videoüberwachung, Wiesbaden 2005.

Steinrötter, B., Kollisionsrechtliche Bewertung der Datenschutzrichtlinien von IT-Dienstleistern – Uneinheitliche Spruchpraxis oder bloßes Scheingefecht?, MMR 2013, 691-694.

Taeger, J./Gabel, D. (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage, Frankfurt am Main 2013.

Tammen, H., Video- und Kameraüberwachung am Arbeitsplatz: Hinweise für Betriebs- und Personalräte, RDV 2000, 15-19.

Thüsing, G., Beschäftigtendatenschutz und Compliance – Effektive Compliance im Spannungsfeld von BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, München 2010.

Thüsing, G., Datenschutz im Arbeitsverhältnis – Kritische Gedanken zum neuen § 32 BDSG, NZA 2009, 865-870.

Tiedemann, K., Datenübermittlung als Straftatbestand, NJW 1981, 945-952.

Timmermann, D./Beigl, M./Handy, M., Prozessoren in Prozessen: Hardware und Dienste für allgegenwärtiges Rechnen, in: Mattern, F. (Hrsg.), Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin Heidelberg 2007, S. 61-77 (zitiert: Bearbeiter, in: Mattern (Hrsg.), Informatisierung des Alltags).

Tinnefeld, M./Buchner, B./Petri, T., Einführung in das Datenschutzrecht – Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Auflage, München 2012.

Tröster, G., Kleidsamer Gesundheitsassistent – Computer am Körper, im Körper, in: Mattern, F. (Hrsg.), Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin Heidelberg 2007, S. 103-127 (zitiert: Bearbeiter, in: Mattern (Hrsg.), Informatisierung des Alltags).

Voigt, P., Internationale Anwendbarkeit des deutschen Datenschutzrechts, ZD 2014, 15-21.

Wandtke, A./Bullinger, W. (Hrsg.), Praxiskommentar zum Urheberrecht, 4. Auflage, München 2014.

Weichert, T., Google Glass, IT-Brillen und informationelle Selbstbestimmung, DANA 2/2013, 53-55.

Weichert, T., Safe Harbor – was ist zu tun?, VuR 2016, 1-3.

Weiser, M., The Computer for the 21st Century, Scientific American, Volume 265, No. 3, S. 94-104. (zitiert: Weiser, Scientific American, 265, 94).

Wright, S./Steventon, A., Smarte Umgebungen – Vision, Chancen und Herausforderungen, in: Mattern, F. (Hrsg.), Informatisierung des Alltags – Leben in smarten Umgebungen, Berlin Heidelberg 2007, S. 17-39 (zitiert: Bearbeiter, in: Mattern (Hrsg.), Informatisierung des Alltags).

Ziegler, P., Blickpunkte – Google Glass vs. Datenschutz, c't 13/2013, 70-71.

Ziegler, P., PC hautnah – Wenn der Computer im Kleiderschrank hängt, c't 21/2002, 102-112.

Internetquellen

Anthony, S., Real-time emotion detection with Google Glass: An awesome, creepy taste of the future of wearable computers, ExtremeTech v. 04.09.2014, http://www.extremetech.com/extreme/189259-real-time-emotion-detection-with-google-glass-an-awesome-creepy-taste-of-the-future-of-wearable-computers (Stand: 28.11.2014).

Bräutigam, T., Itizzimo: Startup Revolutioniert Logistik mit Google Glass, Der Deutsche In-novationspreis v. 02.06.2014, http://www.der-deutsche-innovationspreis.de/das-aktuelle/einzelansicht/article/itizzimo-startup-revolutioniert-logistik-mit-google-glass.html (Stand: 27.11.2014).

DS-GVO, Kompromissentwurf über die Verordnung EU Nr. XXX/2016 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DS-GVO), http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf.

Deutscher Gehörlosen-Bund e. V., Technische Hilfsmittel für Gehörlose, http://www.gehoerlosen-bund.de/index.php?option=com_content&view=article&id=1734%3Atechnischehilfsmittel&catid=107%3Atechnischehilfsmittel&Itemid=153&lang=de (Stand: 13.12.2014)

Eckstein, M., Google Glass – Verkaufsstart bald in Deutschland?, connect v. 28.07.2014, http://www.connect.de/news/google-glass-funktionen-apps-bedienung-1495913.html (Stand 27.11.2014).

Glassware, https://glass.google.com/glassware, (Stand: 04.12.2014); Anmerkung: Seit dem Bekanntwerden des Beenden der Beta-Version Google Glass Anfang Januar, ist die Website nicht mehr in dem vollem Umfang erreichbar. Aufgrund Vollständigkeit und Transparenz wird dennoch auf die entsprechenden Links verwiesen.

Google Glass als Revolution für Behinderte, http://mensch-bruecke.blogspot.de/2013/10/google-glass-eine-revolution-fur.html (Stand: 22.12.2014)

Google Glass Application List, http://glass-apps.org/google-glass-application-list (Stand: 24.01.2015).

Google Glass beim Sport, https://www.google.com/glass/start/what-it-does/ (Stand: 10.01.2015); Anmerkung: Seit dem Bekanntwerden des Beenden der Beta-Version Google Glass Anfang Januar, ist die Website nicht mehr in dem Umfang erreichbar. Aufgrund Vollständigkeit und Transparenz wird dennoch auf die entsprechenden Links verwiesen.

Google Glass, https://www.google.com/glass/start/ (Stand: 04.12.2014); Anmerkung: Seit dem Bekanntwerden des Beenden der Beta-Version Google Glass Anfang Januar, ist die Website nicht mehr in dem Umfang erreichbar. Aufgrund Vollständigkeit und Transparenz wird dennoch auf die entsprechenden Links verwiesen.

Google Glass-App Caption, https://glass.google.com/glassware/1585906026233130545 (Stand: 24.01.2015).

Google Now, http://www.google.com/landing/now/ (Stand: 22.12.2014).

Google Philosophy, www.google.com/about/company/philosophy/ (Stand: 14.01.2015).

Google Street View, https://www.google.com/maps/views/streetview?gl=de&hl=de (Stand: 19.01.2015).

Jawbone Up24, http://jawbone.com/store/buy/up24 (Stand: 04.12.2014).

Költzsch, T., Google Glass für Feuerwehrleute, golem v. 21.01.2014, http://www.golem.de/news/datenbrille-google-glass-fuer-feuerwehrleute-1401-104060.html (Stand: 28.11.2014).

Költzsch, T., Google-Glass-App offiziell in Deutschland verfügbar, golem.de v. 25.07.2014, http://www.golem.de/news/myglass-google-glass-app-offiziell-in-deutschland-verfuegbar-1407-108130.html (Stand: 27.11.2014).

Kramer, A., Erste Fotos der Google Glass 2.0, heise-online v. 29.12.2015, http://www.heise.de/newsticker/meldung/Erste-Fotos-der-Google-Glass-2-0-3056788.html (Stand: 12.01.2016).

Lormis, N., App hilft Autisten bei der Kommunikation, REHACARE.de v. 01.08.2014, http://www.rehacare.de/cipp/md_rehacare/custom/pub/content,oid,35880/lang,1/ticket,g_u_e_s_t/mcat_id,7743/local_lang1 (Stand: 13.12.2014).

Mindsquare, Google Glass und die Lagerlogistik der Zukunft, Mindsquare v. 20.08.2014, http://mindsquare.de/philosophie/news-events/einzelansicht/article/2014/08/20/5/google-glass/ (Stand: 27.11.2014).

MotionSavvy UNI: 1st sign language to voice system, https://www.indiegogo.com/projects/motionsavvy-uni-1st-sign-language-to-voice-system (Stand: 22.12.2014).

MyGlass Support, http://www.google.com/glass/help/myglass/ (Stand: 24.01.2014).

Nocun, K., WolframAlpha: Facebook-Nutzerdaten unter der Statistiklupe – Analysen zu Beziehungsstatus, Interessen und Alter, http://www.netzwelt.de/news/95749-wolframalpha-facebook-nutzerdaten-statistiklupe.html (Stand: 19.01.2015).

Rojahn, S., Google Glass fürs Krankenhaus, Technologie Review v. 21.05.2014, http://www.heise.de/tr/artikel/Google-Glass-fuers-Krankenhaus-2192602.html (Stand: 28.11.2014).

Samsung Galaxy Gear, http://www.samsung.com/de/consumer/mobile-device/wearable/wearable/SM-V7000WDADBT (Stand: 04.12.2014).

Schwenke, T., Vortrag bei der Herbstakademie 2013, http://jurpc52.w2kroot.uni-oldenburg.de/ha13/Schwenke_-_Herbstakademie_2013/14_Schwenke_Google_G_20130912_1711.html (Stand: 09.01.2015).

Spata, O., Polizei von Dubai testet Google Glass, heise-online v. 22.05.2014, http://www.heise.de/newsticker/meldung/Polizei-von-Dubai-testet-Google-Glass-2195634.html (Stand: 28.11.2014).

Sokolov, D., CES 2016: USA erwarten neuen Safe Harbor noch im Januar, heise-online v. 7.1.2016, http://www.heise.de/newsticker/meldung/CES-2016-USA-erwarten-neuen-Safe-Harbor-noch-im-Januar-3064394.html (Stand: 11.1.2016).

Stop the Cyborgs, http://stopthecyborgs.org/ (Stand: 08.01.2015).

Straumann, J., Google Glass nicht für Hörbehinderte – Trotzdem Live-Untertitel für Gehörlo-se und Schwerhörige, HearZone v. 14.07.2014, http://www.hearzone.net/untertitel/1893-google-glass-nicht-f%C3%BCr-h%C3%B6rbehinderte-trotzdem-live-untertitel-f%C3%BCr-geh%C3%B6rlose-und-schwerh%C3%B6rige (Stand: 28.11.2014).

Tätigkeiten der Google Niederlassungen in Hamburg, Berlin, München, http://www.google.com/about/careers/locations/munich/; http://www.google.com/about/careers/locations/hamburg/; http://www.google.com/about/careers/locations/berlin/ (Stand: 22.12.2014).

Terme of Use – Google Glass, http://www.google.com/glass/termsofuse/ (Stand: 21.01.2015).

Tolle Fitness-Apps für Ihr Handy, http://www.computerbild.de/fotos/25-tolle-Fitness-Apps-fuer-Ihr-Handy-6439511.html#1 (Stand: 04.12.2014).

Tung, L., Google Glass owners can now post to Facebook, Twitter, ZDnet v. 17.05.2013, http://www.zdnet.com/google-glass-owners-can-now-post-to-facebook-twitter-7000015533/ (Stand: 27.11.2014).

U.S. – EU Safe Harbor List, https://safeharbor.export.gov/list.aspx (Stand: 19.01.2015).

Wilkens, A., Neustart für Google Glass: Google beendet Verkauf und entwickelt neue Version der Datenbrille, heise-online v. 16.01.2015, http://www.heise.de/newsticker/meldung/Neustart-fuer-Google-Glass-Google-beendet-Verkauf-und-entwickelt-neue-Version-der-Datenbrille-2518518.html (Stand: 16.01.2015).

Zur Gesichtserkennungsfunktion von Google Glass, https://plus.google.com/app/basic/stream/z13zvrmacyntd35z404cinbgmtexjllp5rg0k; https://developers.google.com/glass/policies (Stand: 14.01.2015).

Die vorliegende Masterarbeit setzt sich mit dem aktuellen Rechtsproblem der datenschutzrechtlichen Bewertung von Wearable-Computing-Anwendungen auseinander. An dem Beispiel „Google Glass“ wird untersucht, ob die Privatsphäre und das Recht auf informationelle Selbstbestimmung trotz der Risiken der allgegenwärtigen Datenverarbeitung am menschlichen Körper gewährleistet werden können. Dazu wird analysiert, inwiefern das normative Schutzkonzept des Bundesdatenschutzgesetzes greift und wie die Zulässigkeit der Datenbrille aus datenschutzrechtlicher Sicht zu beurteilen ist. Anhand vier alltäglichen Szenarien wird das Nutzen- und Gefahrenpotenzial von Google Glass datenschutzrechtlich bewertet. Aus den Ergebnissen der juristischen Bewertung werden sodann technische Gestaltungsvorschläge zur Verbesserung der Datenschutzkonformität von Google Glass entwickelt.

ISBN 978-3-7376-0082-8