



universität
wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„Aktueller Stand der Debatte um Bildaufnahmen als
sensible Daten“

verfasst von / submitted by

Mag. Kai Fabian Wieczorrek

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Laws (LL.M.)

Wien, 2024 / Vienna 2024

Studienkennzahl lt. Studienblatt /
Postgraduate programme code as it appears on
the student record sheet:

UA 992 942

Universitätslehrgang lt. Studienblatt /
Postgraduate programme as it appears on
the student record sheet:

Informations- und Medienrecht

Betreut von / Supervisor:

Ao. Univ.-Prof. Dr. iur. Dietmar Jahnel

Abkürzungsverzeichnis

Abkürzungen	Bedeutung
AGB	Allgemeine Geschäftsbedingungen
Art	Artikel
BVwG	Bundesverwaltungsgericht
bzw	Beziehungsweise
DSB	Datenschutzbehörde
DSGVO	Datenschutzgrundverordnung
DSK	Datenschutzkommission
EDSA	Europäische Datenschutzausschuss
EDSB	European Data Protection Board
ErwGr	Erwägungsgrund
etc	Et cetera
EU	Europäische Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
iSd	Im Sinne des
iVm	In Verwendung mit
Meta, Facebook	Meta Platforms Ireland Ltd.
OGH	Oberster Gerichtshof
sog	Sogenannt
ua	Unter anderem
VfGH	Österreichischer Verfassungsgerichtshof
vgl	Vergleiche
zB	Zum Beispiel

1 Inhaltsverzeichnis

2	Einleitung	5
2.1	Ausgangslage	7
2.2	Grundlagen zur datenschutzrechtlichen Verarbeitung von Bildern.....	8
3	Sensible Daten im Sinne der DSGVO	9
3.1	Historische Entstehung des Begriffs.....	9
3.2	Grundrechtliche Zusammenhänge	11
3.3	Besonderheiten für Bilddateien	12
3.3.1	Berücksichtigung in den Erwägungsgründen der DSGVO	13
3.3.2	Exkurs: Regelung im DSG.....	13
4	Diskurs über die Auslegung für Bildaufnahmen	16
4.1	Bisherige Ansätze der Lehre und Praxis zur Einordnung von Bildaufnahmen	16
4.1.1	Subjektiver Ansatz	16
4.1.2	Objektiver Ansatz	19
4.1.2.1	Exkurs: Mischdaten.....	22
4.1.3	Praktische Umsetzung	23
4.2	Judikatur	23
4.2.1	Judikatur: DSB und nationale Gerichte	24
4.2.2	Judikatur: EuGH Entscheidung C-184/20, vom 01.08.2022	25
4.2.2.1	EuGH Entscheidung C-184/20, vom 01.08.2022: Sachverhalt.....	26
4.2.2.2	EuGH Entscheidung C-184/20, vom 01.08.2022: Ausgangsverfahren u Vorlagefrage 27	
4.2.2.3	EuGH Entscheidung C-184/20, vom 01.08.2022: Entscheidung.....	28
4.2.3	Literaturresonanz zu EuGH Entscheidung C-184/20, vom 01.08.2022	30
4.2.3.1	Exkurs: EuG T-557/20 vom 26.04.2023.....	36
4.2.4	Judikatur: EuGH Entscheidung C-252/21, vom 04.06.2023	37
4.2.4.1	EuGH Entscheidung C-252/21, vom 04.06.2023: Ausgangsverfahren u Vorlagefrage 37	
4.2.4.2	EuGH Entscheidung C-252/21, vom 04.06.2023: Entscheidung.....	39
4.2.5	Literaturresonanz zu EuGH Entscheidung C-252/21, vom 04.06.2023	40
4.2.6	Judikatur: EuGH Entscheidung C-667/21, vom 21.12.2023	41
4.2.6.1	EuGH Entscheidung C-667/21, vom 21.12.2023: Ausgangsverfahren u Vorlagefragen 42	
4.2.6.2	EuGH Entscheidung C-667/21, vom 21.12.2023: Entscheidung.....	43
4.2.6.3	Eigene Überlegungen zur EuGH Entscheidung C-667/21, vom 21.12.2023	45
5	Zusammenfassung und Ausblick	46
5.1	Zusammenfassung.....	46

5.2	Mögliche Auswirkungen auf die Praxis	48
5.3	Eigene Interpretation und Ansätze	50
6	Conclusio	55
7	Literaturverzeichnis	57
8	Verzeichnis der Judikatur	60
9	Anhang: Abstract	61

2 Einleitung

Forschungsvorhaben:

Diese Masterarbeit setzt sich mit der Frage auseinander, ob bzw. unter welchen Umständen Bilddateien als sensible Daten iSd des Art 9 DSGVO einzustufen sind. Hierbei soll insbesondere Bezug zur Judikatur des EuGH sowie den herrschenden Theorien der Lehre genommen werden. Darüber hinaus soll ein Ausblick auf die Auswirkungen auf die Praxis gegeben werden.

Forschungsstand:

Lichtbildaufnahmen spielen eine entscheidende Rolle in einer Welt mit fortschreitender Digitalisierung. Problematisch erscheint daher, dass bereits seit der Einführung der DSGVO Rechtsunsicherheit bzw. Auslegungsschwierigkeiten bezüglich der Einordnung von Bilddateien in das Regime der Datenschutzgrundverordnung bestehen, welche zu anhaltenden Diskussionen führen.¹ Insbesondere stellt sich die Frage, ob Bildaufnahmen, welche einen Personenbezug aufweisen, auch als „sensible Daten“ im Sinne der DSGVO anzusehen sind und daher den erhöhten Anforderungen der Verarbeitung unterliegen. Art 9 Abs 1 DSGVO definiert abschließend besondere Kategorien personenbezogener Daten (beispielsweise Gesundheitsdaten oder die religiöse Überzeugung), an deren Verarbeitung strenge Anforderungen gestellt werden.² Dieser Artikel definiert beispielsweise ein grundsätzliches Verarbeitungsverbot und ermöglicht die Verarbeitung nur unter der Einhaltung von sog. „Erlaubnistatbeständen“, welche jedoch restriktiver als die des Art 6 Abs 1 DSGVO (für normale personenbezogene Daten) sind.³ Insbesondere darf die Datenverarbeitung nicht aufgrund einer Abwägung der Interessen erfolgen.

Bisher wird in der Datenschutzpraxis sowie einem Teil der Lehre die Ansicht vertreten, dass auf den Zweck der Bildverarbeitung bzw. auf den Kontext der Verarbeitung abzustellen sei, um beurteilen zu können, ob sensible Daten verarbeitet werden.⁴

Demgegenüber ist ein Teil der Lehre der Ansicht, dass die Qualifikation eines Datums als sensibles Datum nach rein objektiven Maßstäben zu erfolgen hat.⁵ Eine solche Auslegung könnte jedoch beispielsweise zu dem Problem führen, dass Bildaufnahmen von einer Person, die ein Kopftuch oder eine Brille trägt, als Verarbeitung von sensiblen Daten angesehen werden könnten.

¹ Vgl. etwa *Jahnel*, DSB: Bilddaten als nicht-sensible Daten, *jusIT* 2019/32, 89 (89).

² Siehe *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim* (Hrsg.), *DatKomm Art 9 DSGVO Rz 1* (Stand 7.5.2020, *rdb.at*).

³ Siehe *Sedef/Steiner*, Datenverarbeitung, *Lexis Briefings in lexis360.at*.

⁴ Vgl. *Thiele/Wagner*, EU-DSGVO: Umsetzung der DSGVO in der Personalpraxis (2019) 54.

⁵ Vgl. *Bergauer*, Die Einordnung von Bilddaten erkennbarer Personen im Datenschutzrecht. Eine Replik auf *Knyrim*, Bilddaten: immer sensibel?, *jusIT* 2016/103, 241 (246).

Der EuGH hat sich in seiner bisherigen Judikatur nicht eindeutig zur Einordnung von Bildern als sensible Daten geäußert. Die Entscheidung C-184/20 des EuGH vom 01.08.2022 nimmt jedoch explizit Bezug zur Auslegung des Begriffs „sensible Daten“ und ist daher auch für die Beurteilung von Bilddateien von Bedeutung.

In dieser Entscheidung wird eine weite Auslegung der Definition „besonderer Kategorien personenbezogener Daten“ postuliert.⁶ Um den hohen Schutzzweck der DSGVO gewährleisten zu können, müssen gemäß dieser Auslegung daher auch Daten, welche indirekt sensible Informationen über eine natürliche Person offenbaren können, dem erhöhten Schutz des Art 9 Abs 1 DSGVO unterliegen. Da die Entscheidung keinen Bezug auf einen möglichen Verwendungszweck bzw andere subjektive Kriterien der Verarbeitung nimmt, könnte dieses Judikat als Ablehnung der oben beschriebenen Theorie verstanden werden.⁷

Laimighofer nahm die gegenständliche Entscheidung zum Anlass, einen eigenen Ansatz zu den Auswirkungen dieser Entscheidung für die Verarbeitung von Bilddateien zu formulieren.⁸ Eine weite Auslegung des Begriffs der sensiblen Daten und eines damit verbundenen hohen Schutzniveaus könnte in der Praxis, insbesondere bei der Verarbeitungen von Bildaufnahmen, weitreichende Folgen haben.⁹ Verweist doch beispielsweise die WKO in ihrer Musterformulierung für Veranstaltungen auf das berechnete Interesse des Veranstalters gemäß Art 6 Abs 1 lit f DSGVO Bildaufnahmen erheben und veröffentlichen zu können.¹⁰

Diese Masterarbeit verfolgt das Ziel, die aktuelle Debatte der oben beschriebenen Problematik darzustellen sowie mögliche Theorien zu finden um die vorherrschenden Ansätze mit der aktuellen Judikatur zu harmonisieren.

Forschungsfrage:

- Lässt sich die jüngste Judikatur des EuGH mit den bisher herrschenden Theorien bezüglich der Einstufung von Bilddateien als sensible Daten vereinbaren? Bzw lässt diese Raum für neue Auslegungsweisen?

⁶ Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 125f.

⁷ Vgl. Gosch, Zur Reichweite der Klassifizierung sensibler Daten, *jusIT* 2022/76, 183 (186).

⁸ Siehe Laimighofer, Was macht Fotos zu sensiblen Daten?, *jusIT* 2023/43, 102 (102).

⁹ Vgl. Kienle, Vorlage zur Vorabentscheidung – Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, *LTZ* 2023, 50 (67).

¹⁰ Siehe <wko.at/branchen/information consulting/werbung-marktkommunikation/fotografie-und-werbung.html> (12.11.2023).

2.1 Ausgangslage

Digitale Daten bestimmen für viele Menschen nicht nur den privaten Alltag, sondern darüber hinaus auch die berufliche Tätigkeit. So verfügen beispielsweise mehr als 90% der Unternehmen in Österreich über eine eigene Website und über 65% nutzen Soziale Medien im beruflichen Kontext.¹¹ Diese voranschreitende Entwicklung wird immer intensiver und in der Folge auch zu einer steigenden Verarbeitung von Daten beitragen. So gehen Schätzungen davon aus, dass die allgemeine Datenflut dazu führen wird, dass sich die Menge an jährlich erzeugten bzw replizierten Daten in dem Zeitraum von 2017 bis 2027 mehr als verzehnfachen wird.¹² Durch diese Erhöhung der Datenverarbeitungen wird auch die Anzahl an Verarbeitungen jener Daten mit Personenbezug zunehmen. Dies ist insbesondere auch für das Datenschutzrecht relevant, da eine Erhöhung der Verarbeitungen zum einen ein höheres Risiko für die Rechtmäßigkeit der Verarbeitungen darstellt und zum anderen spezielle Einzelfälle auch die Judikatur vor neue Herausforderungen stellen können. Abseits davon berührt der Bildnisschutz und die damit im Zusammenhang stehenden Verarbeitungen eine Vielzahl an Rechtsgebieten.¹³

Insbesondere Bilddateien bzw deren Einordnung in das Europäische Datenschutzrecht waren bereits in der Vergangenheit Diskussionsgegenstand der Lehre.¹⁴ Umso dringlicher erscheint eine eindeutige Einordnung der Verarbeitung von Bilddateien vor dem Hintergrund steigender Technologisierung, wie beispielsweise der Verwendung von sogenannten „KI-Anwendungen“.¹⁵ So gaben in einer Studie, welche durch Statistik Austria im Jahr 2021 durchgeführt wurde, rund ein Viertel der Unternehmen, welche „KI-Technologien“ benutzten, an, dass sie diese neuartigen Technologien zur Bilderkennung oder Verarbeitung verwenden würden.¹⁶ Sollte es sich bei diesen Anwendungsfällen beispielsweise auch um Videoüberwachungen handeln, welche Aufnahmen von Personen verarbeiten, würde sich aus datenschutzrechtlicher Sicht vermutlich die Hauptfrage dieser Arbeit stellen: „Sind Bilddateien als sensible Daten im Sinne der DSGVO anzusehen?“

¹¹ Siehe *Statistik Austria*, IKT-EINSATZ IN UNTERNEHMEN (2021), <statistik.at/fileadmin/publications/IKT_Unternehmen_2021.pdf> (28.07.2023).

¹² Siehe <de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen> (28.07.2023).

¹³ Löw, „Bildnisschutz“: Absoluter Schutz vor unbefugtem Veröffentlichen von Lichtbildern?, ZIIR 2023, 142 (142).

¹⁴ Siehe *Jahnel*, jusIT 2019/32, 89 (90).

¹⁵ Anmerkung: in der Wissenschaft herrscht Uneinigkeit in welchem Zusammenhang von einer KI, also künstlichen Intelligenz, gesprochen werden kann.

¹⁶ Siehe *Statistik Austria*, IKT-EINSATZ IN UNTERNEHMEN (2021), Tabelle A.29.

2.2 Grundlagen zur datenschutzrechtlichen Verarbeitung von Bildern

Bevor auf die speziellen Besonderheiten sowie die konkrete Einordnung von Bilddateien in das Europäische Datenschutzrecht eingegangen werden kann gilt es die Grundlagen der Verarbeitung von Bildaufnahmen kurz darzustellen. Welche Bildaufnahmen, bzw dessen Verarbeitungen, sollen von der DSGVO erfasst sein?

Der räumliche Anwendungsbereich der DSGVO wird in Art 3 DSGVO bestimmt. Im Wesentlichen sind sämtliche Verarbeitungen von personenbezogenen Daten erfasst, welche von einer Niederlassung eines Verantwortlichen bzw eines Auftragsverarbeiters in der EU (im Rahmen ihrer Tätigkeit) verarbeitet werden.¹⁷ Darüber hinaus sind auch solche Verarbeitungen von personenbezogenen Daten durch nicht in der EU niedergelassene Verantwortliche oder Auftragsverarbeiter erfasst, sofern sich die betroffene Person in der EU befindet.¹⁸ Als sachlicher Anwendungsbereich der DSGVO gibt Art 2 DSGVO die Verarbeitung von personenbezogenen Daten vor, unabhängig davon, ob die entsprechende Verarbeitung automatisch oder manuell erfolgt. Die in Art 4 Z 2 DSGVO gefasste Definition von „Verarbeitung“ ist hierbei weit zu verstehen, laut *Hödl* sollen alle datenschutzrechtlich relevanten Vorgänge in Bezug auf personenbezogene Daten erfasst sein.¹⁹ Der „Personenbezug“ der Daten im Sinne der DSGVO setzt weiters voraus, dass es sich lediglich um Daten einer natürlichen (lebenden) Person handeln kann.²⁰

Die Darstellung der entsprechenden Daten ist weiters unbeachtlich und kann aus diesem Grund durch verschiedene Medien erfolgen, solange die auf diese Weise dargestellte Datei entweder automatisch, teilautomatisch oder manuell in einem Datensystem verarbeitet werden.²¹ Zusätzlich müssen sich solche Daten auf eine identifizierte bzw identifizierbare Person beziehen.²² Die Identifizierbarkeit wird in Art 4 Z 1 DSGVO definiert. Die Identifikation kann hierbei direkt oder indirekt erfolgen, zur genaueren Auseinandersetzung dieser Bestimmung, insbesondere der indirekten Identifizierung, wird an dieser Stelle auf das Kapitel 4.2.3 dieser Arbeit verwiesen.

Das Speichern, Bearbeiten, Löschen etc einer Bildaufnahme kann beispielsweise eine Verarbeitung von personenbezogenen Daten im Sinne der DSGVO darstellen. Dies jedoch unter der Voraussetzung, dass es sich hierbei um eine Bildaufnahme einer lebenden, erkennbaren natürlichen Person

¹⁷ Siehe Art 3 Abs 1 DSGVO.

¹⁸ Siehe Art 3 Abs 2 DSGVO.

¹⁹ Siehe *Hödl* in Knyrim (Hrsg), *DatKomm* (2018) Art 4 DSGVO Rz 25 (Stand 1.12.2018, rdb.at).

²⁰ Siehe Art 4 Z 1 DSGVO.

²¹ Siehe *Bergauer* in Jähnel (Hrsg), *Kommentar zur Datenschutz-Grundverordnung* Art 4 Z 1 DSGVO Rz 11 (2021).

²² Siehe Art 4 Z 1 DSGVO.

handelt.²³ Für den Personenbezug im Sinne der DSGVO genügt es laut *Hödl*, dass die Erkennbarkeit zumindest nachträglich besteht.²⁴ Bei Bildaufnahme im privaten Bereich ist insbesondere die sogenannte „Haushaltsausnahme“ zu berücksichtigen. Gemäß Art 2 Abs 2 lit c DSGVO sind Verarbeitungen durch natürliche Personen vom Anwendungsbereich der DSGVO ausgenommen, wenn sie zur Ausübung von „ausschließlich persönlichen oder familiären Tätigkeiten“ dienen. Daher sind zB auch private Familienfotos oder ähnliche Lichtbildaufnahmen nicht vom Anwendungsbereich der DSGVO erfasst.²⁵ Nicht der Anwendung des Haushaltsprivilegs unterliegen jedoch beispielsweise Videoüberwachungsaufnahmen, wenn durch die Überwachungskamera – auch nur teilweise – der öffentliche Raum überwacht wird.²⁶ Für die Anwendbarkeit dieser Ausnahme ist es des Weiteren unbeachtlich, um welche Datenkategorie es sich handelt. Von der Haushaltsausnahme sind sowohl „normale“ als auch sensible personenbezogene Daten erfasst.²⁷

Grundsätzlich hat jede Verarbeitung von personenbezogenen Daten, sofern sie in den Anwendungsbereich der DSGVO fällt, den Anforderungen gemäß Art 5 DSGVO zu entsprechen und als zusätzliche Bedingung einen der Rechtfertigungsgründe des Art 6 Abs 1ff DSGVO zu erfüllen, um rechtmäßig zu sein. Sonderbestimmungen bestehen für sogenannte sensible Daten, auf welche im folgenden Kapitel genauer eingegangen wird.

3 Sensible Daten im Sinne der DSGVO

3.1 Historische Entstehung des Begriffs

Auch wenn der Begriff der „sensiblen Daten“ im datenschutzrechtlichen Sprachgebrauch weit verbreitet ist, ist es überraschend, dass im Text der DSGVO diese Bezeichnung darin keine direkte Verwendung findet. In der deutschen Sprachfassung lässt zwar Erwägungsgrund 10 die Verwendung des besagten Terminus erhoffen, allerdings handelt es sich hierbei um die einzige Erwähnung dieser Begrifflichkeit.²⁸ Ähnlich verhält es sich in der Richtlinie 95/46/EG (sog Datenschutzrichtlinie), welche salopp formuliert die Vorgängerbestimmung der DSGVO darstellt. Auch in besagter Richtlinie finden „sensible Daten“ bzw „sensible Datenkategorien“ lediglich Erwähnung in den Erwägungsgründen. Beschrieben werden soll mit diesem Begriff die, für den gewöhnlichen Sprachgebrauch etwas sperrig anmutende, Formulierung „Verarbeitung besonderer Kategorien personenbezogener Daten“ im Sinne

²³ Siehe *Bergauer* in DSGVO Art 4 Z 1 DSGVO Rz 16.

²⁴ Siehe *Hödl* in DatKomm Art 4 DSGVO Rz 16.

²⁵ Siehe *Bergauer* in DSGVO Art 4 Z 1 DSGVO Rz 24.

²⁶ Siehe *Hödl* in DatKomm Art 4 DSGVO Rz 69; Vgl *Bergauer* in DSGVO Art 4 Z 1 DSGVO Rz 28.

²⁷ Siehe *Bergauer* in DSGVO Art 4 Z 1 DSGVO Rz 25.

²⁸ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1 idF ABl L 2021/74, 35.

des Art 9 DSGVO bzw des Art 8 Datenschutzrichtlinie. Die Bezeichnungen werden seither synonymhaft verwendet.

Aus dem Wortlaut des Begriffs „Verarbeitung besonderer Kategorien personenbezogener Daten“ ergibt sich, dass im Gegensatz zu „normalen“ personenbezogenen Daten auch solche Daten existieren, welche einer „besonderen Kategorie“ angehören. Insofern werden für die Verarbeitung von personenbezogenen Daten, je nachdem welchen „Kategorien“ sie angehören, unterschiedliche Anforderungen gestellt.

Bereits in der Datenschutzrichtlinie wurde ein taxativer Katalog an Kategorien definiert, an dessen Verarbeitung besondere Maßstäbe zu setzen sind. Die Datenschutzrichtlinie (deren Umsetzung den Mitgliedstaaten oblag) sah daher ein Verbot zur Verarbeitung von personenbezogenen Daten vor, aus denen „[...] *die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben*“.²⁹ Die Definition dieser besonderen Kategorien an Daten ist im Wesentlichen deckungsgleich mit den sogenannten „besonderen Datenarten“, wie sie bereits in Art 17 des Richtlinienvorschlags aus dem Jahr 1990 angegeben waren.³⁰ Insofern liegt diesen besonderen Kategorien eine gewisse Beständigkeit der letzten Jahrzehnte zugrunde.

In weiterer Folge sah Art 8 Abs 2 RL 95/46/EG Ausnahmen vor, welche die Verarbeitung der besagten personenbezogenen Daten (sensible Daten) unter gewissen Voraussetzungen bzw für bestimmte Zwecke ermöglichen sollte. Beispielhaft kann hier die Einwilligung des Betroffenen, arbeitsrechtliche Verpflichtungen des Verantwortlichen sowie jene Fälle, in denen sich die Datenverarbeitung auf Daten bezieht, welche von der betroffenen Person öffentlich gemacht wurden, genannt werden.

Das Pendant zu dem oben beschriebenen Artikel der Datenschutzrichtlinie findet sich in der DSGVO in Art 9 und orientiert sich sehr stark an seiner Vorgängerbestimmung.

Als meines Erachtens in diesem Zusammenhang nennenswerteste Änderung kann die Ergänzung um die Verarbeitung von genetischen Daten sowie „*biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person*“ genannt werden. Aufgrund der zunehmenden technischen Entwicklungen, welche automatisierte Auswertungen (beispielsweise durch die Verwendung von Algorithmen) von biometrischen Daten ermöglichen, wurde diese Kategorie ergänzt.³¹ Zusätzlich kann darauf hingewiesen werden, dass die Datenschutzrichtlinie bereits aufgrund der gewählten Rechtsform die

²⁹ Siehe Art 8 Abs 1 RL 95/46/EG.

³⁰ Siehe KOM(90) 314 endg.-SYN 287-288.

³¹ Siehe *Kastelitz/Hötzendorfer/Tschohl* in *DatKomm* Art 9 DSGVO Rz 146.

Mitgliedstaaten adressierte. Durch die DSGVO sind nunmehr neben den Mitgliedstaaten auch die Normadressaten selbst unmittelbar von dem europäischen Rechtsakt erfasst.

3.2 Grundrechtliche Zusammenhänge

Wie zuvor beschrieben, besteht eine Art „Sonderbehandlung“ für Daten, die den besonderen Arten an Datenkategorien der DSGVO zugeordnet werden können. Dies wird besonders durch das grundsätzliche Verbot der Verarbeitung, welches Art 9 Abs 1 DSGVO vorgibt, bestimmt. Insofern bestehen daher für sensible Daten strengere Anforderungen an die Verarbeitung als für „reguläre“ personenbezogene Daten.³² Auch die Ausnahmen, welche eine Verarbeitung von sensiblen Daten rechtfertigen, sind weniger weit formuliert als es bei „normalen“ personenbezogenen Daten der Fall ist. Anders als bei der Verarbeitung von normalen personenbezogenen Daten gemäß Art 6 Abs 1 ff DSGVO existierten für die Verarbeitung von sensiblen Daten weder der Rechtfertigungsgrund aufgrund der Erfüllung eines Vertrags noch kann eine Verarbeitung aufgrund eines überwiegenden Interesses des Verantwortlichen oder eines Dritten erfolgen. Diese Unterscheidung wurde nicht neu durch die DSGVO eingeführt, sondern bestand bereits in der Datenschutzrichtlinie.³³

Gründe für eine solche Unterscheidung bei der Verarbeitung von verschiedenen Arten von personenbezogenen Daten werden unter anderem in Erwägungsgrund 51 der DSGVO gegeben. Bereits im ersten Satz dieses Erwägungsgrunds erfolgt der Hinweis auf das erhebliche Risiko, bezogen auf die Grundrechte und Grundfreiheiten, welches sich aus einer Verarbeitung dieser Datenkategorien ergeben könnte.³⁴ Die Artikel-29-Datenschutzgruppe führte dazu 2011 weiters aus, dass durch die Verarbeitung bzw durch einen entsprechenden Missbrauch von Daten dieser besonderen Kategorien ein sehr hohes Schadenspotential bestehen würde.³⁵ So könnte beispielsweise eine missbräuchliche Verwendung von sensiblen Daten, welche zB die Offenlegung der sexuellen Orientierung betreffen, für den Betroffenen unumkehrbar sein und lange anhaltende Folgen nach sich ziehen. Insofern wird seitens der Artikel-29-Datenschutzgruppe darauf hingewiesen, dass die missbräuchliche Verarbeitung von sensiblen Daten besondere Auswirkungen auf das Grundrecht der Nicht-Diskriminierung sowie auf das Recht auf Privatsphäre haben kann.³⁶

³² Siehe *Schmidbauer*, Begriff und Verarbeitung sensibler Daten in der Judikatur des EuGH, *jusIT* 2023/32, 66 (67).

³³ Siehe *Kastelitz/Hötzendorfer/Tschohl* in *DatKomm* Art 9 DSGVO Rz 1.

³⁴ Siehe ErwGr 27 VO (EU) 2016/679.

³⁵ Siehe *Artikel-29-Datenschutzgruppe*, Advice paper on special categories of data (“sensitive data”), Ref Ares (2011) 444105, 4 <ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf> (22.01.2024).

³⁶ Siehe *Artikel-29-Datenschutzgruppe*, Ref Ares (2011) 444105, 4.

Bereits unter Erwägungsgrund 1 der DSGVO wird das Grundrecht des Schutzes natürlicher Personen bei der Verarbeitung von personenbezogenen Daten postuliert. In weiterer Folge, insbesondere auch in der einschlägigen Judikatur des EuGH,³⁷ wurde der Schutz der Grundrechte und Grundfreiheiten bzw die Wahrung und Schaffung eines möglichst hohen Niveaus dieser als Leitmaxime der DSGVO definiert. Ebenso bestimmt Art 1 Abs 2 DSGVO den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen als einer der Grundausrichtungen der DSGVO.³⁸ Diese Bestimmung ist daher von hoher Bedeutung für die Auslegung der anderen Artikel der gesamten Verordnung.³⁹

Insofern ist das Datenschutzrecht von seinem Grundgedanken aus eng mit den Grundrechten verbunden. In diesem Zusammenhang stellen die Bestimmungen des Art 9ff DSGVO einen zusätzlichen Ausdruck dieses Grundrechtsgedanken dar. In Erwägungsgrund 4 der DSGVO wird klargestellt, dass auch das „Recht auf Schutz der personenbezogenen Daten“ kein uneingeschränktes Recht darstellt. Es sei vielmehr erforderlich, dieses Recht unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte entsprechend abzuwägen. Die Umsetzung dieses Verhältnismäßigkeitsprinzips spiegelt sich meines Erachtens in der Ausgestaltung des Art 9 DSGVO wider.⁴⁰ Der Gesetzgeber hat die Verarbeitung von Daten dieser besonderen Kategorien bereits im Vorfeld als möglicherweise besonders intensiven Eingriff eingestuft bzw ein besonders hohes Schadenspotenzial bei missbräuchlicher Verwendung dieser Datenkategorien ermittelt. Insofern kann dies als Ausdruck eines „risikobasierten Ansatzes“ verstanden werden.⁴¹

3.3 Besonderheiten für Bilddateien

Ganz allgemein gesprochen kann es sich bei der Verarbeitung von Bilddateien um eine Verarbeitung von personenbezogenen Daten im Sinne der DSGVO handeln. Hierbei ist entscheidend, was auf dem Bild dargestellt wird, bzw welche Daten es beinhaltet.

Gemäß dem Anwendungsbereich der DSGVO ist daher ein Personenbezug erforderlich.⁴² Eine Person muss daher zumindest durch das Bild identifizierbar sein, damit ein Lichtbild ein personenbezogenes Datum darstellt. Durch das auf einem Bild Gezeigte lassen sich jedoch in der Regel verschiedene Informationen ableiten. Insbesondere kann in vielerlei Fällen Rückschluss auf die rassisch / ethnische Herkunft, die religiöse Überzeugung oder den Gesundheitszustand einer Person gezogen werden.⁴³ In

³⁷ Vgl EuGH 06.11.2003, C-101/01 (Lindqvist); EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija).

³⁸ Siehe *Lachmayer* in Knyrim (Hrsg), *DatKomm Art 1 DSGVO Rz 6* (Stand 1.12.2018, rdb.at).

³⁹ Vgl *Lachmayer* in *DatKomm Art 1 DSGVO Rz 25*.

⁴⁰ Vgl *Frenzel* in Paal/Pauly (Hrsg), *DS-GVO BDSG³ Art 9 DSGVO Rz 1* (2021).

⁴¹ Siehe *Schulz* in Gola/Heckmann (Hrsg), *Datenschutz-Grundverordnung - Bundesdatenschutzgesetz³ Art 9 DSGVO Rz 2* (2022); *Schiff* in Ehmann/Selmayr (Hrsg), *Datenschutz-Grundverordnung² Art 9 DSGVO Rz 1* (2018).

⁴² Siehe Art 2 Abs 1 DSGVO, Art 4 Abs 1 DSGVO.

⁴³ Siehe *Knyrim*, *Bilddaten: immer sensibel?*, *jusIT* 2016/102, 235 (236).

einem ersten Schritt wird daher in dieser Arbeit zu prüfen sein, ob sich in der DSGVO sowie dem österreichischen DSG besondere Regelungen für die Verarbeitung von Bilddateien finden.

3.3.1 Berücksichtigung in den Erwägungsgründen der DSGVO

Dass Bilddateien, als besonderes Medium für Informationen, komplexen Überlegungen bezüglich ihrer Beurteilung im Bereich des Datenschutzrechts bedürfen, ergibt sich unter anderem bereits aus den rechtlich unverbindlichen Erwägungsgründen der DSGVO.

Erwägungsgrund 51 der DSGVO nimmt explizit Bezug auf Lichtbilder und führt weiters dazu aus, dass diese „[...] *nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden* [...]“ sollten. In weiterer Folge wird darauf Bezug genommen, dass Lichtbilder nur unter der Voraussetzung, dass sie mit „speziellen technischen Mitteln“ verarbeitet werden, unter die Definition der „biometrischen Daten“ fallen würden. Diese „speziellen technischen Mittel“ würden die eindeutige Identifizierung und Authentifizierung einer natürlichen Person ermöglichen.⁴⁴

Bereits in der Vergangenheit war der oben genannte Erwägungsgrund ein wichtiger Anhaltspunkt für die mögliche Einordnung der Verarbeitung von Lichtbildern.⁴⁵ Unklar blieb, ob sich die Aussage, dass es sich bei der Verarbeitung von Lichtbildern grundsätzlich um keine Verarbeitung von sensiblen Daten handeln würde, lediglich auf die Definition von biometrischen Daten bezieht, daher nicht jede Verarbeitung von Bilddateien eine Verarbeitung von biometrischen Daten darstellt und gar keine generelle Aussage zur Qualifikation von Lichtbildern als sensible Daten getroffen werden wollte.⁴⁶

Man könnte den Erwägungsgrund allerdings auch dahingehend verstehen, dass die DSGVO zwischen regulären Bildern und solchen, welche biometrische Informationen einer Person verarbeiten sollen, unterscheidet.⁴⁷ In weiterer Folge wurde unter anderem der hier thematisierte Erwägungsgrund und die zuletzt genannte Interpretation als Indiz herangezogen, dass für die Einordnung von Datenverarbeitungen in die Kategorie der sensiblen Daten auch die subjektive Absicht des Datenverarbeiters ausschlaggebend ist. Dies steht im Gegensatz zur objektiven Betrachtungsweise.⁴⁸ Auf die weitere Beurteilung und Einordnung dieses Ansatzes wird in 4.1.1 genauer eingegangen.

3.3.2 Exkurs: Regelung im DSG

Wie sich bereits aus den zuvor genannten Punkten ergibt, besteht insbesondere auch in der Praxis ein hohes Interesse daran, Bildaufnahmen datenschutzrechtlich möglichst eindeutig einordnen zu

⁴⁴ Siehe ErwGr 51 VO (EU) 2016/679.

⁴⁵ Siehe *Kastelitz/Hötzendorfer/Tschohl* in *DatKomm* Art 9 DSGVO Rz 18/1.

⁴⁶ Siehe *Knyrim*, *jusIT* 2016/102, 235 (239).

⁴⁷ Siehe beispielsweise *Knyrim*, *jusIT* 2016/102, 235 (239).

⁴⁸ Zur Gegenüberstellung von objektiver und zweckberücksichtigender Betrachtung siehe beispielsweise *Gosch*, *jusIT* 2022/76, 183 (186).

können. Veranschaulichen lässt sich dies an dem in der Praxis immer wieder relevanten Beispiel der Videoüberwachung durch Dashcams. Für entsprechende Bildverarbeitungen für private Zwecke sieht das österreichische DSG – im Gegensatz zu den Bestimmungen der DSGVO – eigene Regelungen vor. Die entsprechenden Regelungen finden sich in § 12 DSG sowie § 13 DSG. Wobei letztgenannter besondere Anforderungen an die Datensicherungsmaßnahmen und an die Verarbeitung von Bilddateien stellt.

§ 12 Abs 1 DSG beinhaltet eine eigene, weitgefasste Definition von Bildaufnahmen, in welcher auch akustische Signale inkludiert sind, und gibt darüber hinaus Voraussetzungen vor, unter welchen die Bildverarbeitung zulässig ist. Durch diese Regelung wird eine grundsätzliche Vereinheitlichung der Verarbeitung von Bilddateien angestrebt.⁴⁹ Diese Norm richtet sich jedoch lediglich an Bildverarbeitungen, welche zu „privaten Zwecken“ erfolgen. „Private Zwecke“ sind in diesem Zusammenhang als Gegenstück zu öffentlichen Zwecken zu verstehen, insofern sollen auch berufliche Aufnahmen vom Anwendungsbereich der Norm erfasst sein, sofern diese nicht ohnedies unter die sogenannte Haushaltsausnahme der DSGVO fallen.⁵⁰

Diese Regelung erfasst auch Verarbeitungen durch Verantwortliche des öffentlichen Bereichs, wenn diese im Rahmen der Privatwirtschaftsverwaltung handeln.⁵¹ In § 12 Abs 2 DSG werden Erlaubnistatbestände taxativ aufgezählt sowie in Abs 3 eine Interessenabwägung vorgenommen. Des Weiteren werden in § 12 Abs 4 DSG Verbote definiert, so ist beispielsweise die Verarbeitung von Bilddateien des höchstpersönlichen Lebensbereichs ohne ausdrückliche Einwilligung unzulässig. Neben der Überwachung von Arbeitnehmer:innen ist beispielsweise auch die Auswertung von personenbezogenen Daten, welche von Bildaufnahmen entnommen wurden, unzulässig, wenn für die Auswertung besondere Kategorien personenbezogener Daten als Auswahlkriterium herangezogen werden.

Die in § 12 Abs 2 DSG aufgezählten Erlaubnistatbestände entsprechen bzw ähneln den Erlaubnistatbeständen des Art 6 und Art 9 DSGVO.⁵² Die Verarbeitung von Bildaufnahmen gemäß dieses Paragraphen ist, unter Einhaltung von in § 13 DSG bestimmten „Besondere Datensicherheitsmaßnahmen und Kennzeichnung“, zulässig, wenn sie aufgrund von lebenswichtigen Interessen einer Person erforderlich ist, eine Einwilligung der betroffenen Person besteht, die Verarbeitung aufgrund von besonderen gesetzlichen Bestimmungen angeordnet oder erlaubt ist oder

⁴⁹ Siehe *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG)² § 12 DSG Rz 9 (2022).

⁵⁰ Siehe AB 1761 BlgNR XXV. GP 8.

⁵¹ Siehe *Thiele/Wagner*, DSG² § 12 Rz 12.

⁵² Siehe *Pollirer et al*, DSG⁴ § 12 Rz 4f (Stand 1.4.2019, rdb.at).

aber im Einzelfall das überwiegende Interesse des Verantwortlichen oder eines Dritten besteht sowie die Verhältnismäßigkeit gewahrt ist.⁵³

Diese zuvor beschriebene nationale Regelung der Verarbeitung von Bilddateien stützt der Gesetzgeber auf Öffnungsklauseln der DSGVO (Art 6 Abs 2 und 3 sowie Art 23 DSGVO und Kap IX DSGVO iVm ErwGr 10).⁵⁴ Wie bereits in der Vorgängerbestimmung soll hierdurch eine gesonderte Regelung der Bildverarbeitung auch im DSG, unter Berücksichtigung der Erfahrungen aus der Vergangenheit, erfolgen.⁵⁵ Die praktische Anwendung dieser Bestimmungen ist jedoch äußerst eingeschränkt. In diversen Entscheidungen des BVwGs vertritt dieser die Ansicht, dass § 12 und § 13 DSG aufgrund Ermangelung einer zulässigen Öffnungsklausel in der DSGVO unangewendet zu bleiben haben.⁵⁶

Zusätzlich wurde die EuGH-Entscheidung vom 11.12.2019, C-708/18, von der österreichischen Datenschutzbehörde zum Anlass genommen, ihre Anwendungspraxis betreffend der gegenständlichen Bestimmungen des DSG zu ändern.⁵⁷ Seither beschränkt die DSB die Rechtmäßigkeitsprüfung der Bildverarbeitung auf die einschlägigen Artikel 5 und 6 der DSGVO und lässt § 12ff DSG unangewendet.⁵⁸ Demgegenüber weist *Jahnel* darauf hin, dass in einigen Entscheidungen, des Obersten Gerichtshofs (OGH 27.11.2019, 6 Ob 150-19f sowie OGH 20.05.2020 6 Ob 206/19s), sehr wohl von der Anwendbarkeit der entsprechenden österreichischen Bestimmungen ausgegangen wurde. Eine endgültige Klärung der Frage der Anwendbarkeit dieser Normen wird erst die weitere Entwicklung der Rechtsprechung ergeben.⁵⁹ Insofern besteht eine Judikaturdivergenz zwischen den Entscheidungen des BVwG und des OGH.

Die Relevanz dieser Bestimmung des DSG bleibt damit für die Praxis ungewiss. *Thiele* u *Wager* vertreten trotz der Spruchpraxis des BVwG die Ansicht, dass kein durchgängiger Anwendungsnachrang für die §§ 12 und 13 DSG bestehen würde und begründen dies mit der deutschen Spruchpraxis, bei welcher die private Videoüberwachung ausschließlich aufgrund berechtigten Interesses (Art 6 Abs 1 lit f DSGVO) geprüft werden würde. Dies käme im Wesentlichen der Prüfungslogik von § 12 Abs 2 Z 4 DSG gleich.⁶⁰ Des Weiteren führen *Thiele* u *Wagner* aus, dass im Falle der Bewertung von Bildaufnahmen als sensible Daten Art 9 Abs 2 lit g DSGVO als

⁵³ Siehe § 12 Abs 2 DSG.

⁵⁴ Siehe AB 1761 BlgNR XXV. GP 8.

⁵⁵ Siehe AB 1761 BlgNR XXV. GP 8.

⁵⁶ Siehe beispielsweise BVwG 25.11.2019, W211 2210458-1; BVwG 20.11.2019, W256 2214855-1; siehe *Thiele/Wagner*, DSG² § 12 DSG Rz 128.

⁵⁷ Siehe *Panic/Wolf*, Änderungen im Bereich der Bilddatenverarbeitung, MR 2020 Heft 1, 3 (4).

⁵⁸ Siehe *Feiler/Forgó*, EU-DSGVO² § 12 DSG Rz 1 (2022).

⁵⁹ Siehe *Jahnel*, Kommentar zur Datenschutz-Grundverordnung (DSGVO) Art 6 DSGVO Rz 89 (2021).

⁶⁰ Siehe *Thiele/Wagner*, DSG² § 12 DSG Rz 129.

Öffnungsklausel geprüft werden könnte. Aufgrund eines „erheblichen öffentlichen Interesses“ könnte zB § 12 Abs 4 DSG, welcher regelt wann eine Bildaufnahme unzulässig ist, demzufolge unionsrechtskonform und damit anzuwenden sein.⁶¹

Bisher, Stand November 2023, konnte sich in der Judikatur keine einheitliche Line zur Anwendung der in diesem Abschnitt diskutierten Bestimmungen des DSG herausbilden. Spätestens durch die Aufhebung des sogenannten „Medienprivilegs“ (§ 9 Abs 1 DSG) durch den VfGH⁶² ergibt sich meines Erachtens, dass einige der österreichischen Datenschutzbestimmungen auf juristisch „wackligen Beinen“ stehen.

4 Diskurs über die Auslegung für Bildaufnahmen

4.1 Bisherige Ansätze der Lehre und Praxis zur Einordnung von Bildaufnahmen

Dass Bildaufnahmen von Personen ein besonderes Medium darstellen, mit welchem personenbezogene Daten verarbeitet werden, lässt sich gut durch die Worte des EuGH beschreiben. Dieser sprach in seiner Entscheidung vom 08.12.2022, C-460/20, wie folgt aus: *„Das Bild eines Einzelnen ist nämlich eines der Hauptmerkmale seiner Persönlichkeit, da es seine Einmaligkeit zum Ausdruck bringt und es erlaubt, ihn von anderen Personen zu unterscheiden.“*⁶³

Auch wenn dieses Zitat eine Entscheidung betrifft, welche sich nicht mit der Kategorisierung von Bilddateien als sensible Daten auseinandersetzt, so zeigt dieses doch meines Erachtens den hohen Stellenwert, welchen der EuGH an den Schutz des eigenen Bildes einer Person setzt. Dennoch werden Lichtbilder, welche einen Personenbezug aufweisen nicht per se als sensible Daten qualifiziert, obwohl diese Bilddateien auch sensible Daten beinhalten können (beispielsweise Gesundheitsdaten).⁶⁴ Zur Klärung dieser Unklarheiten haben sich in der österreichischen Literatur im Wesentlichen zwei verschiedene Theorien entwickelt, welche in Folge genauer behandelt werden sollen.

4.1.1 Subjektiver Ansatz

Die erste, gemäß *Laimighofer*⁶⁵ in der österreichischen Literatur vorherrschende Theorie stützt sich auf eine subjektive, an dem Zweck orientierende Herangehensweise der Qualifikation von Bilddateien als sensible Daten. Insbesondere *Knyrim* vertritt diese Ansicht und begründete dies im Wesentlichen damit, dass Daten erst durch das Hinzutreten einer subjektiven Auswertung sensible Daten

⁶¹ Siehe *Thiele/Wagner*, DSG² § 12 DSG Rz 130.

⁶² Siehe VfGH 14.12.2022, G 287/2022, G 288/2022.

⁶³ Siehe EuGH 8.12.2022, C-460/20 (Google) Rz 95.

⁶⁴ Siehe *Laimighofer*, jusIT 2023, 102 (102).

⁶⁵ Siehe *Laimighofer*, jusIT 2023, 102 (102).

hervorbringen.⁶⁶ In einem hierzu 2016 veröffentlichten Artikel beschrieb *Knyrim* diesen Vorgang am Beispiel von körperlichen Merkmalen von Personen. Diese Informationen könnten jeweils von verschiedenen Personen für verschiedene Zwecke verwendet werden. Zum einen könnten die körperlichen Merkmale auf eine mögliche Erkrankung schließen lassen bzw auf den Gesundheitszustand einer Person Rückschlüsse erlauben. Auf der anderen Seite könnten solche Informationen, wie zB die Körpergröße einer Person, auch für weniger eingriffsintensive Zwecke verwendet werden, wie etwa der Feststellung der Kleidergröße.⁶⁷

Diese Überlegungen könnten gemäß *Knyrim* in weiterer Folge auch auf Bilddateien angewendet werden. Da Bildaufnahmen grundsätzlich zuerst einmal eine Aneinanderreihung von Dateninformationen wären, bedürfte es einer Interpretation bzw Auswertung dieser Informationen. Diese könne auch durch alltägliche Informationen erfolgen und ließe beispielsweise den Rückschluss zu, dass ein Brillenträger eine Sehschwäche (Gesundheitsdatum) aufweisen würde. Eine solche Verarbeitung würde in der Regel vollautomatisch über unser Unterbewusstsein erfolgen.⁶⁸ Darüber hinaus wird ins Treffen geführt, dass bei einer Nichtberücksichtigung des Verarbeitungszwecks einem Verarbeiter stets unterstellt werden könnte, dass er Daten, aus denen sich auch sensible Daten auswerten ließen, welche dem besonderen Schutz des Art 9 DSGVO unterliegen, verarbeitet.⁶⁹

Des Weiteren wird der bereits unter 3.3.1 angeführte Erwägungsgrund 51 der DSGVO zur Unterstützung der Argumentation herangezogen. *Knyrim* vertritt die Ansicht, dass sich über den ErwGr 51 der DSGVO ableiten lässt, dass die Verarbeitung von Bilddateien nicht allgemein als Verarbeitung von sensiblen Daten anzusehen ist, solange keine speziellen technischen Mittel verwendet werden würden, um gezielt sensible Daten aus dem Bildmaterial auszuwerten.⁷⁰ Der hier angeführten Theorie folgend, vertritt auch *Schulz* in der bundesdeutschen Literatur die Ansicht, dass für die Beurteilung, ob Art 9 DSGVO anzuwenden ist, eine kontextabhängige Betrachtung erforderlich ist, welche von der Auswertungsabsicht des Verantwortlichen stark bestimmt wird.⁷¹

Andere Sichtweisen, welche „verobjektiviert“ von einer Verarbeitung von sensiblen Daten allein deshalb ausgehen, sofern sich schutzwürdige Informationen mit „hinlänglicher Sicherheit“ ableiten ließen, würden zu einer bedenklichen „Aufblähung“ des Anwendungsbereichs von Art 9 DSGVO führen. Eine solche Auslegung würde zudem den Telos der Norm aus den Augen verlieren. Die

⁶⁶ Siehe *Knyrim*, jusIT 2016/102, 235 (237).

⁶⁷ Siehe *Knyrim*, jusIT 2016/102, 235 (236ff).

⁶⁸ Siehe *Knyrim*, jusIT 2016/102, 235 (237f).

⁶⁹ Siehe *Knyrim*, jusIT 2016/102, 235 (238).

⁷⁰ Siehe *Knyrim*, jusIT 2016/102, 235 (239).

⁷¹ Siehe *Schulz* in DS-GVO / BDSG³ Art 9 DSGVO Rz 13.

besonderen Schutzmaßnahmen („Sondervorschriften“) seien daher im Zweifelsfall nicht anwendbar.⁷² Auch *Schiff* misst dem Verarbeitungszweck des Verantwortlichen Bedeutung zu, verweist jedoch darauf, dass bei deutlichem Vorliegen von objektiven Anzeichen einer Verarbeitung von sensiblen Daten die Prüfung des subjektiven Verwendungszwecks in den Hintergrund zu treten hat.⁷³ Ebenso ist *Frenzel* der Überzeugung, dass manchen Daten eine gewisse Doppelfunktionalität innewohnt: beispielsweise könnten Daten in „Alltagsgeschäften“ zur Identifikation einer Person verwendet werden oder aber, um die Herkunft („Ethnie“) einer Person zu bestimmen. Entscheidend sei daher eine Verbindung von den entsprechenden Daten mit einer bestimmten Verarbeitung, damit diese unzulässig ist. Dem Zweck käme daher auch der Meinung *Frenzel* folgend entscheidende Bedeutung zu.⁷⁴ Seiner Ansicht nach müsste diese erfassbare subjektive Zwecksetzung jedoch objektiviert werden und in der Folge die Beurteilung der Verarbeitung im Einzelfall erfolgen. Hierzu sollte die Beurteilung der Datenverarbeitung in beide Richtungen, zu Gunsten und zu Lasten des Verantwortlichen sowie des Betroffenen, berücksichtigt werden.⁷⁵

Dem hier beschriebenen „subjektiven Ansatz“ kann jedoch, wie beispielsweise *Frenzel* selbst, entgegengehalten werden, dass im Wortlaut der DSGVO eine Anknüpfung an den Kontext, welcher „normale“ Daten zu sensiblen Daten werden lässt, nicht angelegt ist.⁷⁶

Dennoch gibt es einige Anzeichen dafür, dass auch der Europäische Datenschutzausschuss (EDSA) eine Beurteilung anhand des Verarbeitungszwecks bevorzugt. In seinem Leitfaden 3/2019 beschäftigte sich der EDSA mit der „Verarbeitung von personenbezogenen Daten durch Videogeräte“.

In einem eigenen Abschnitt wird auch die Verarbeitung von besonderen Kategorien personenbezogener Daten berücksichtigt. Zwar wird grundsätzlich darauf hingewiesen, dass durch Videoüberwachung eine große Menge an personenbezogenen Daten verarbeitet wird und dies auch sensible Daten umfassen könnte, jedoch würde nicht jede Videoüberwachung auch eine Verarbeitung von besonderen Kategorien personenbezogener Daten darstellen. Hierfür wird als Beispiel angeführt, dass nicht jede Videoaufnahme, welche eine betroffene Person mit einer Brille oder in einem Rollstuhl sitzend zeigt, grundsätzlich eine Verarbeitung von sensiblen Daten darstellen würde.⁷⁷ Als entscheidendes Kriterium wird geprüft, ob das Videomaterial dafür verarbeitet werden würde, um

⁷² Siehe *Schulz* in DS-GVO / BDSG³ Art 9 DSGVO Rz 13.

⁷³ Siehe *Schiff* in DS-GVO² Art 9 DSGVO Rz 18.

⁷⁴ Siehe *Frenzel* in DS-GVO BDSG³ Art 9 DSGVO Rz 9.

⁷⁵ Siehe *Frenzel* in DS-GVO BDSG³ Art 9 DSGVO Rz 9.

⁷⁶ Siehe *Frenzel* in DS-GVO BDSG³ Art 9 DSGVO Rz 9.

⁷⁷ Siehe *EDSA*, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.1, Rz 62f <edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_de.pdf> (22.01.2024).

sensible Daten daraus ableiten zu können.⁷⁸ Gemäß *Jahnel* bleibt die EDSA jedoch in ihrem Leitfaden eine Erklärung schuldig, woher sich diese Argumentation aus der DSGVO ableiten ließe.⁷⁹ *Laimighofer* merkt kritisch an, dass die Erwägungen des Europäischen Datenschutzausschusses aus rein praktischen Gründen so getroffen worden seien.⁸⁰ Führt der EDSA doch unter der Rz 70 aus, dass „[...] *wahrscheinlich kaum eine der in Artikel 9 aufgeführten Ausnahmen dazu genutzt werden kann, die Verarbeitung besonderer Datenkategorien durch Videoüberwachung zu rechtfertigen.*“

Dennoch besitzt diese Auslegungsweise in der deutschen Literatur viele Anhänger. Hierbei wird beispielsweise darauf verwiesen, dass durch das bloße Aufnehmen von Videomaterial durch Überwachungskameras noch keine besonderen Risiken der Betroffenen entstehen würden, die eine Anwendung des Art 9 Abs 1 DSGVO rechtfertigen würden, sofern die Daten nur über einen Bildschirm angezeigt bzw später wieder gelöscht werden würden. Entscheidend sei die Auswertungsabsicht des Verarbeiters, welche darauf abstellen würde, dass durch Videoaufnahmen eine Auswertung der Informationen im Sinne des Art 9 Abs 1 DSGVO erfolgen soll. Für Verarbeitungen, welche ohne solche Auswertungsabsicht erfolgen würden, könne daher auf Art 6 DSGVO zurückgegriffen werden. Eine gewisse Nähe zu den Datenkategorien der sensiblen Daten könne beispielsweise bei der Prüfung der Verhältnismäßigkeit der Verarbeitungen entsprechend berücksichtigt werden.⁸¹ Sollten durch Videoaufnahmen daher Angaben im Sinne des Art 9 Abs 1 DSGVO ableitbar bzw diese Daten unmittelbar im Bildmaterial enthalten sein, jedoch ohne Vorliegen einer Auswertungsabsicht verarbeitet werden, lägen *Schneider* und *Schindler* folgend keine besonderen Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen vor, weshalb die Anwendbarkeit der besonderen Bestimmungen des Art 9 Abs 1 DSGVO nicht erforderlich seien.⁸²

4.1.2 Objektiver Ansatz

Einer subjektiven bzw an den Verarbeitungszweck orientierten Zuordnung von Daten zu den sensiblen Kategorien kann eine stärker objektive Auslegungsweise entgegengehalten werden. Für die Beurteilung von Daten als sensible Daten nach objektiven Kriterien wird als Argumentation auch eine der grundsätzlichen Zielsetzungen der DSGVO herangezogen: die Schaffung eines möglichst hohen Datenschutzniveaus.⁸³

⁷⁸ Siehe EDSA, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Rz 64.

⁷⁹ Siehe *Jahnel*, Kommentar zur Datenschutz-Grundverordnung (DSGVO) Art 9 DSGVO Rz 24 (2021).

⁸⁰ Siehe *Laimighofer*, *jusIT* 2023, 102 (103).

⁸¹ Siehe *Schneider/Schindler*, Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten, *ZD* 2018, 463 (467).

⁸² Siehe *Schneider/Schindler*, *ZD* 2018, 463 (468).

⁸³ Siehe *Bergauer*, *jusIT* 2016/103, 241 (245).

Diesem „objektiven Interpretationsspektrums“ angehörend, vertritt *Jahnel* beispielsweise die Meinung, dass der Wortlaut des Art 9 DSGVO nahelegen würde, dass sich die konkrete Zuordnung von Daten zu den besonderen Datenkategorien an objektiven Maßstäben zu orientieren hätte.⁸⁴ Dem Wortlaut des Art 9 sowie der Systematik der DSGVO wäre weiters nicht zu entnehmen, dass der Verwendungszusammenhang oder der subjektive Zweck eines Verarbeiters berücksichtigt werden könnten.⁸⁵ Die Zulässigkeit der Datenverarbeitung und die Zuordnung der Daten zu den verschiedenen Datenkategorien sei streng zu trennen.

So würden zB in die Interessenabwägung gemäß Art 6 Abs 1lit f DSGVO („normale“ Daten) sehr wohl der subjektive Verarbeitungszweck des Verarbeiters einfließen, dies wäre aber eine Frage der Zulässigkeit der Verarbeitung.⁸⁶ Bei der Zuordnung der Daten zu den jeweiligen Kategorien könne laut *Jahnel* niemals die „subjektive Intention des Verarbeiters“ als zulässiges Kriterium herangezogen werden.⁸⁷

Im Gegensatz dazu sei eine Berücksichtigung des Verwendungszusammenhangs (objektiver Kontext) der Verarbeitung, je nach „Typus der besonderen Datenkategorie“ teilweise zwingend erforderlich.⁸⁸ *Jahnel* unterscheidet hierbei aufgrund des Wortlauts des Art 9 Abs 1 DSGVO zwischen drei verschiedenen Typen von sensiblen Daten:

Zum einen gäbe es solche Daten, die „an sich“ sensibel wären. Dies beträfe die Kategorien genetische Daten, Gesundheitsdaten, Daten zum Sexualleben sowie der sexuellen Orientierung. Wenn die jeweilige Begriffsbestimmung erfüllt ist, soll es sich bei Daten dieser Kategorien um sensible Daten handeln.⁸⁹

Bei dem zweiten Typus, den sogenannten „Hervorgehens-Daten“ (Daten der Kategorien rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie Gewerkschaftszugehörigkeit), komme es aufgrund des Wortlauts darauf an, ob aus den verarbeiteten Daten diese Informationen „hervorgehen“.⁹⁰ Aufgrund dieses Begriffs bestünde gemäß *Jahnel* eine gewisse Flexibilität bei der Zuordnung, was eine Berücksichtigung des Verwendungszusammenhangs ermöglichen würde.⁹¹ Bei diesem Typus soll es weiters bereits ausreichen, dass sich die sensiblen Informationen aus den konkreten Daten ableiten bzw folgern lassen. Begrenzt wird diese

⁸⁴ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 12.

⁸⁵ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 12.

⁸⁶ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 13.

⁸⁷ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 14.

⁸⁸ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 14.

⁸⁹ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 15.

⁹⁰ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 15.

⁹¹ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 15.

Ableitbarkeit der Informationen dadurch, dass sich die „sensiblen Informationen“ mit „hinlänglicher Sicherheit“ aus den vorhandenen Daten ableiten lassen müssen.⁹² *Bergauer* führt als Beispiel an, dass ein Bild, welches eine Person vor einer Kirche zeigen würde, noch nicht ausreichend wäre, um etwa auf die religiöse Orientierung einer Person schließen zu lassen, folglich würde es sich um kein sensibles Datum handeln. Das Kriterium der „hinlänglichen Sicherheit“ sei jedoch bei „Doppeldeutigkeit“ zu verneinen.⁹³ *Gosch* sieht eine solche Auslegung potenziell dem Schutzzweck der DSGVO sowie der Judikatur des EuGH entgegenstehend (siehe weiter unter 4.2.3).⁹⁴ Diese einschränkende Interpretation des Wortes „hervorgehen“ würde sich laut *Jahnel* noch aus dem Wortlaut des Art 9 DSGVO ableiten lassen.⁹⁵ Auch *Schiff* verwendet eine ähnliche Formulierung und stellt auf das Kriterium der „hinreichenden Wahrscheinlichkeit“ ab, misst jedoch (siehe unter 4.1.1) auch dem Verarbeitungszweck Bedeutung für die Beurteilung von sensiblen Daten zu.⁹⁶

Als letzter Typus würden laut *Jahnel* die biometrischen Daten eine gewisse Sonderstellung einnehmen. Diese müssten zur eindeutigen Identifizierung einer natürlichen Person verwendet werden, daher würde in diesem Fall ein eindeutiger Bezug auf den Verwendungszusammenhang genommen werden.⁹⁷

Ob eine solche Unterscheidung in verschiedene Typen und eine darin liegende tiefere Bedeutung aus dem Wortlaut des Verordnungstextes ableitbar ist, wurde in der Vergangenheit auch teils kritisch betrachtet. Insbesondere aufgrund der Mehrsprachigkeit, welche in der EU besteht, könnten „sprachliche Feinheiten“ nicht immer aufschlussreich sein.⁹⁸

Laut *Bergauer* sei jedoch grundsätzlich bereits die Berücksichtigung des Verwendungszusammenhangs – ebenso wie die des Verwendungszwecks – nicht mit der DSGVO zu vereinbaren. Dies leitet er unter anderem daraus ab, dass Art 9 Abs 1 DSGVO für biometrische Daten den Zusatz „zur eindeutigen Identifizierung einer natürlichen Person“ enthält und insofern auf den Zweck der Verwendung der biometrischen Daten abstellt. Daraus könne geschlossen werden, dass grundsätzlich „[...] die Einordnung von sensiblen Informationen unter die anderen von Art 9 Abs 1 DSGVO berücksichtigten Datenarten nicht anhand des konkreten Verwendungszusammenhangs zu erfolgen hat, sondern nach objektiven Gesichtspunkten.“⁹⁹ Darüber hinaus ist *Bergauer* der Meinung, dass ErwGr 51 DSGVO – welcher von Befürwortern der Berücksichtigung des subjektiven

⁹² Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 21.

⁹³ Siehe *Bergauer*, jusIT 2016/103, 241 (246).

⁹⁴ Siehe *Gosch*, jusIT 2022/76, 183 (187).

⁹⁵ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 22.

⁹⁶ Siehe *Schiff* in DS-GVO² Art 9 DSGVO Rz 14.

⁹⁷ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 15.

⁹⁸ Vgl *Schneider/Schindler*, ZD 2018, 463 (467).

⁹⁹ Siehe *Bergauer*, jusIT 2016/103, 241 (244f).

Verarbeitungszwecks häufig herangezogen wird¹⁰⁰ – ausschließlich Bezug auf die Definition des Begriffs „biometrische Daten“ nimmt. Daraus würde sich ableiten lassen, dass nicht jede Lichtbildaufnahme auch ein biometrisches Datum darstelle, sondern hierfür zusätzlich eine informationstechnische Verarbeitung zu Identifizierungszwecken erforderlich sei.¹⁰¹ Seiner Ansicht folgend, solle einzig aufgrund von objektiven Gesichtspunkten geprüft werden, ob Informationen (beispielsweise auch Bilddateien) als sensible Daten kategorisiert werden können.¹⁰² Als Begrenzung, um ein Überschießen zu verhindern, sei gemäß *Bergauer* lediglich das Kriterium der „hinlänglichen Sicherheit“ statthaft.¹⁰³

Kritik wird jedoch auch an dieser Auslegungsweise geäußert, da auch eine Subsumtion unter Begriffen wie „hinlängliche Sicherheit“ bzw. „objektiv wahrscheinlich“ zu Rechtsunsicherheit führen und für die Praxis zu keiner sonderlichen Erleichterung beitragen würde.¹⁰⁴ *Laimighofer* bezweifelt, dass das Kriterium der „hinlänglichen Sicherheit“ einen Mehrwert und eine Einschränkung gegenüber dem Begriff des „Hervorgehens“ des Art 9 Abs 1 DSGVO darstellt. Ebenso wie aus einer Bildaufnahme, bei der eine Person vor einer Kirche zu sehen ist, nicht mit „hinreichender Sicherheit“ auf seine religiöse Ausrichtung geschlossen werden kann, würde aus einem solchen Bildnis auch schlicht gar nicht eine solche Information „hervorgehen“.¹⁰⁵ Seiner Argumentation folgend, würde der Begriff des „Hervorgehens“ dieselben Voraussetzungen erfüllen: etwas würde sich zwar nicht direkt ergeben, könnte sich aber daraus ableiten lassen. Eine bloße Vermutung sei jedoch nicht ausreichend, damit eine solche Information aus etwas „hervorgeht“.¹⁰⁶

4.1.2.1 Exkurs: Mischdaten

In dem gegenständlichen Kontext wird auch der Begriff der sogenannten „Mischdaten“ verwendet.¹⁰⁷ Hierbei handelt es sich um Daten, welche sich nicht zweifelsfrei einer Kategorie („besondere Kategorie personenbezogener Daten“ oder „normale“ personenbezogene Daten) zuordnen lassen.¹⁰⁸ *Jahnel* definiert Mischdaten als „[...] eine Sammlung an Informationen, die eine Gemengelage von nicht-sensiblen und sensiblen personenbezogenen Daten enthält oder die aus mehreren verschiedenen besonderen Kategorien personenbezogener Daten und anderen personenbezogenen Daten, die keiner besonderen Kategorie angehören, besteht.“¹⁰⁹ *Bergauer* vertritt die Ansicht, dass die Verarbeitung

¹⁰⁰ Siehe etwa *Knyrim*, *jusIT* 2016/102, 235 (239).

¹⁰¹ Siehe *Bergauer*, *jusIT* 2016/103, 241 (245).

¹⁰² Siehe *Bergauer*, *jusIT* 2016/103, 241 (246).

¹⁰³ Siehe *Bergauer*, *jusIT* 2016/103, 241 (246).

¹⁰⁴ Vgl. *Matejek/Mäusezahl*, *Gewöhnliche vs. sensible personenbezogene Daten*, *ZD* 2019, 551 (553).

¹⁰⁵ Siehe *Laimighofer*, *jusIT* 2023, 102 (106).

¹⁰⁶ Siehe *Laimighofer*, *jusIT* 2023, 102 (106).

¹⁰⁷ Vgl. *Jahnel*, *DSGVO Art 9 DSGVO Rz 29*.

¹⁰⁸ Siehe *Brodil*, *Datenschutz und Arbeitsrecht* (2018) 3.

¹⁰⁹ Siehe *Jahnel*, *DSGVO Art 9 DSGVO Rz 29*.

von Mischdaten (dies umfasst beispielsweise auch Bildaufnahmen) dem Schutzregime der am schutzwürdigsten Information unterliegen soll.¹¹⁰ Weiters verweist er darauf, dass sich die Problematik von Mischdaten insbesondere am Beispiel von Gesundheitsdaten auf Bildaufnahmen zeigen würde. So könnten quasi aus jedem Bild, welches erkennbar eine natürliche Person zeigt, auch Gesundheitsdaten gewonnen werden (zB Brillenträger, Narben, etc).¹¹¹ Schulz ist der Ansicht, dass durch den Verantwortlichen aufgrund einer subjektiven Entscheidung, der Zweck der Datenverarbeitung bestimmt wird. Diese Entscheidung würde sich auch darauf beziehen, ob aus „Mischdatensätzen“ sensible Bestandteile eines Datums verarbeitet werden sollen.¹¹²

4.1.3 Praktische Umsetzung

Die beiden zuvor dargestellten Ansätze (sowie ihre entsprechenden Variationen) verdeutlichen meines Erachtens die Uneinheitlichkeit, welche bisher in der Literatur zur Einordnung von Informationen als sensible Daten besteht.

Da allerdings in der Praxis ein Bedürfnis besteht, ua Bilddateien – auf denen auch natürliche Personen erfasst sind – zu verarbeiten, wurde regelmäßig auf die „verarbeitungsfreundlichere“ Auslegung, welche auf den Verarbeitungszweck (subjektiver Ansatz) abstellt, zurückgegriffen.¹¹³ Entsprechend verweist auch beispielsweise die Wirtschaftskammer Österreich in einem Leitfaden für die Anfertigung von Videoaufnahmen bei Veranstaltungen, auf die Rechtfertigungsgründe des Art 6 Abs 1ff DSGVO, ohne auf die Thematik betreffend sensibler Daten Bezug zu nehmen.¹¹⁴ Unter Punkt 5.2 dieser Arbeit werden die weiteren Auswirkungen der jüngsten Judikatur des EuGH auf die aktuelle Praxis dargestellt.

4.2 Judikatur

Wie zuvor aufgezeigt, divergieren die Lehrmeinungen bezüglich der Einordnung von Bilddateien als sensible Daten. Erschwerend kommt zu dieser Problematik hinzu, dass die österreichische Datenschutzbehörde sowie nationale Gerichte in der Vergangenheit Entscheidungen getroffen haben, welche möglicherweise schwierig mit der jüngsten Judikatur des EuGH zu vereinbaren sind. In der Folge sollen daher ausgewählte Entscheidungen zur Verdeutlichung der Problematik skizziert werden.

¹¹⁰ Siehe *Bergauer*, *jusIT* 2016/103, 241 (244).

¹¹¹ Siehe *Bergauer*, *jusIT* 2016/103, 241 (246).

¹¹² Siehe *Schulz* in *DS-GVO / BDSG*³ Art 9 DSGVO Rz 13.

¹¹³ Vgl *Hense*, *Informationsaskese vs. Meta - Perspektiven des EuGH auf datengetriebene Praktiken in der modernen Gesellschaft*, *KuR* 2023, 556 (559).

¹¹⁴ Siehe <wko.at/branchen/information consulting/werbung-marktkommunikation/fotografie-und-werbung.html>.

4.2.1 Judikatur: DSB und nationale Gerichte

Die DSB beschäftigte sich in der Vergangenheit mehrfach mit der Frage, ob Bildaufnahmen als Verarbeitung von sensiblen Daten zu betrachten sind und vereinte dies, wie *Jahnel* ausführte, ohne jegliche Begründung.¹¹⁵ Zu diesen Entscheidungen der DSB zählen etwa die Folgenden:

In einem Verfahren, in welchem die Antragstellerin im Zuge eines Forschungsprojekts, Bildaufnahmen der Straßenoberflächen bzw des Straßenraums anfertigen wollte (auf diesen Bildaufnahmen wären „unvermeidbar“ auch Verkehrsteilnehmer:innen ersichtlich), entschied die DSB, dass mit der Verarbeitung dieser Bilddateien keine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art 9 Abs 1 DSGVO vorliegen würde.¹¹⁶ Mit dieser Entscheidung reiht sich die DSB im Wesentlichen in die Spruchpraxis der DSK (Vorgänger der DSB) ein. Bei ähnlich gelagerten Fällen, welche noch vor Inkrafttreten der DSGVO angesiedelt waren, wurde beispielsweise Verkehrsteilnehmer:innen die sensible Eigenschaft bei der Verarbeitung von Lichtbildern nicht zuerkannt.¹¹⁷ In einer weiteren Entscheidung aus dem Jahr 2020, bestätigte die DSB diese Rechtsansicht unter Verweis auf die zuvor genannte Entscheidung aus dem Jahr 2018.¹¹⁸ In einer ähnlichen Entscheidung (Forschungsprojekt für autonome Fahrzeuge) aus dem Jahr 2023, verwies die DSB erneut auf die bereits erwähnten Entscheidungen, formuliert meines Erachtens jedoch etwas vorsichtiger, dass mit diesen Bilddateien „im Regelfall“ keine Verarbeitung von sensiblen Daten vorliegen würde.¹¹⁹

Eine weitere Entscheidung der DSB beschäftigte sich mit der Anfertigung und dem Abgleich von Lichtbildern zur Zugangskontrolle eines Skilifts bzw des Skigebiets. Der Fotoabgleich sollte, gemäß der Beschwerdegegnerin, missbräuchliche Verwendungen der Skipässe verhindern. Die DSB entschied, dass die Verarbeitung durch die Beschwerdegegnerin gemäß Art 6 Abs 1 lit f DSGVO gerechtfertigt gewesen sei.¹²⁰ Bezüglich der Frage, ob es sich bei der Verarbeitung der Lichtbilder um eine Verarbeitung von besonderen Kategorien personenbezogener Daten handeln könnte, argumentierte die DSB, dass Lichtbilder nur dann in diese Kategorien fallen können, wenn sie von der Begriffsdefinition „biometrische Daten“ erfasst wären. Zu dieser Beurteilung kommt die DSB unter Verweis auf den unter Punkt 4.1.1 genauer beschriebenen Leitfaden der EDSA zur Verarbeitung personenbezogener Daten durch Videogeräte. Weiters verweist die DSB auf den Erwägungsgrund 51 der DSGVO und das darin geregelte Erfordernis der Verarbeitung von Lichtbildern mit „speziellen

¹¹⁵ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 23.

¹¹⁶ Siehe DSB 07.06.2018, DSB-D202.207/0001-DSB/2018.

¹¹⁷ Vgl *Thiele/Wagner*, DSG² § 12 Rz 54.

¹¹⁸ Siehe DSB 21.01.2020, DSB 2020-0.013.649.

¹¹⁹ Siehe DSB 21.06.2023, DSB 2022-0.930.971.

¹²⁰ Vgl *Haidinger/Löffler*, Geheimhaltung: Zutrittskontrolle mittels Fotoabgleich, *Dako* 2023/12, 20; *Thiele*, DSB: Zutrittskontrolle bei Skiliftanlagen, *jusIT* 2022/52, 116 (116f).

technischen Mittel“, um von dem Begriff „biometrische Daten“ erfasst zu sein.¹²¹ Die DSB fasst die Thematik zusammen wie folgt: *„Ein einfaches digitales Foto, das wie hier nur zu optischen Vergleichszwecken gespeichert und auf einem Bildschirm angezeigt wird, ohne „speziellen technischen Verfahren“ unterzogen zu werden, erfüllt daher keinen Tatbestand der Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO.“*¹²²

Aus diesem Zitat ergibt sich meines Erachtens, dass die DSB für die Beurteilung, ob mit einer Lichtbildaufnahme auch sensible Daten verarbeitet werden, auch auf den Verwendungszweck der gespeicherten und anders verarbeiteten Daten abstellt. Anders wäre unter Umständen die Entscheidung ausgefallen, wenn die Beschwerdeführerin die Daten nicht „nur zu optischen Vergleichszwecken“ verarbeitet hätte. Die DSB folgt damit meines Erachtens den Überlegungen, wie sie etwa von *Knyrim* definiert wurden.

Auch in der österreichischen (Höchst-) Judikatur zeichnet sich ein ähnliches Bild ab, so wird durch den BVwG die Prüfung der Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten bei Aufnahmen von Lichtbildern regelmäßig nur anhand von Art 6 Abs 1 lit f DSGVO geprüft.¹²³ Auf die Frage, ob durch solche Verarbeitungen auch sensible Daten, wie beispielsweise die „Rasse oder ethnische Herkunft“ einer Person, verarbeitet werden, wird meines Erachtens nicht genauer eingegangen. In einer anderen Entscheidung des BVwG, welcher die Anfertigung und Übermittlung eines Fotos eines „Maskenattests“ (Stichwort: „Gesundheitsdatum“) zugrunde lag, wurde diese Bildaufnahme als Verarbeitung sensibler Daten im Sinne der DSGVO eingestuft.¹²⁴ Jedoch ist hierbei darauf hinzuweisen, dass nicht auf die Thematik eingegangen wurde, ob auch eine Bildaufnahme der „Krankheitssymptome“ der betroffenen Person eine solche Datenverarbeitung darstellen würde.

4.2.2 Judikatur: EuGH Entscheidung C-184/20, vom 01.08.2022

Wie bereits durch *Jahnel* beschrieben, liegt es neben dem europäischen Gesetzgeber in der Hand des EuGH für Klarheit in der Problematik bezüglich der sensiblen Daten zu sorgen.¹²⁵ Zu dem Begriff der sensiblen Daten äußerte sich der EuGH erstmals in der Entscheidung „Lindqvist“ aus dem Jahr 2003.¹²⁶ Hierbei berief sich der europäische Gerichtshof auf den Zweck der damals relevanten Datenschutzrichtlinie, welcher gewesen sei, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.¹²⁷ In der Folge legte der EuGH den Begriff der Gesundheitsdaten weit aus.¹²⁸

¹²¹ Siehe DSB 23. 11. 2020, 2020-0.759.615.

¹²² Siehe DSB 23. 11. 2020, 2020-0.759.615 7.

¹²³ Vgl etwa BVwG 11.07.2023, W108 2250460-1; BVwG 21.04.2023, W245 2246467-1.

¹²⁴ Siehe BVwG 28.07.2023, W245 2245697-1.

¹²⁵ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 26.

¹²⁶ Siehe *Schmidbauer*, *jusIT* 2023/32 2023, 66 (67).

¹²⁷ Siehe EuGH 6. 11. 2003, C-101/01 (Lindqvist) Rz 95.

Abschließend geklärt wurde durch diese und in den Jahre darauf folgende Judikatur die Frage der Auslegung von sensiblen Daten jedoch nicht.

Aus diesem Grund soll in dem folgenden Kapitel auf zwei Entscheidungen der jüngeren Vergangenheit eingegangen werden, welche meines Erachtens wichtige Erkenntnisse zu der bisher geführten Diskussion bringen. Auch hierbei steht die Schaffung eines möglichst hohen Schutzniveaus im Fokus der Judikatur des EuGH. Wichtig ist dabei darauf hinzuweisen, dass sich diese Entscheidungen nicht unmittelbar mit der Frage der Einordnung von Bilddateien als sensible Daten auseinandersetzen, sich aber auch auf die „Lichtbilder-Problematik“ übertragen lassen.

4.2.2.1 EuGH Entscheidung C-184/20, vom 01.08.2022: Sachverhalt

Der Sachverhalt des Ausgangsverfahrens der Entscheidung C-184/20 des EuGH vom 01.08.2022 kann im Wesentlichen wie folgt zusammengefasst werden: Der Beschwerdeführer ist Leiter einer öffentlichen Einrichtung, welche sich mit Themen des Umweltschutzes auseinandersetzt.¹²⁹ In Litauen ist des Weiteren ein Gesetz in Kraft, welches unter anderem der Korruptionsbekämpfung dienen soll. Personen, welche im öffentlichen Dienst tätig sind, sollen bei ihrer Entscheidungsfindung öffentlichen Interessen den Vorrang gegenüber den eigenen Interessen geben und möglichst unparteilich vorgehen. Der Beschwerdeführer fällt als Person, welche im öffentlichen Dienst tätig ist, in den Anwendungsbereich dieses Gesetzes. Um diese beschriebenen Ziele zu verwirklichen, fordert das Gesetz von Personen, welche in seinen Anwendungsbereich fallen, dass sie ihre persönlichen Interessen offenlegen müssen. Im Zuge dessen, muss die betroffene Person eine Erklärung über ihre Interessen abgeben. Diese Erklärung umfasst verschiedenste Informationen, welche neben Daten wie der Sozialversicherungsnummer sowie Unternehmensbeteiligungen, auch beispielsweise Angaben zu Geschenken, welche innerhalb der letzten zwölf Monate erhalten wurden und einen Wert von mehr als EUR 150,- aufweisen sowie Informationen über abgeschlossene und laufende Transaktionen der letzten zwölf Monate, welchen einen Wert von mehr als EUR 3.000,- umfassen. Die Verpflichtung zur Abgabe dieser Angaben trifft jedoch nicht nur die erklärungspflichtige Person, sondern zusätzlich sind die entsprechenden Angaben auch bezüglich Ehegatt:innen, Lebensgefährte:innen oder Partner:innen abzugeben. Zuständig für die Entgegennahmen und Kontrolle dieser Erklärungen ist die sogenannte „Oberste Ethikkommission“. Diese hat für die Umsetzung des Gesetzes zu sorgen. Darüber hinaus hat die Oberste Ethikkommission, in Umsetzung des Gesetzes, die erhaltenen Daten auf ihrer Website der Öffentlichkeit zugänglich zu machen. Ausnahmen bestehen jedoch unter anderem für die

¹²⁸ Siehe *Schmidbauer*, *jusIT* 2023/32 2023, 66 (67); *Kronegger*, *EuGH „Lindqvist“: Datenschutz im Internet, Medien und Recht* 2004, 83 (83).

¹²⁹ Siehe *EuGH* 01.08.2022, C-184/20 (*Vyriausioji tarnybinės etikos komisija*) Rz 36f.

Sozialversicherungsnummer sowie besondere personenbezogene Daten oder auch Daten, deren Offenlegung gesetzlich verboten ist.

4.2.2.2 *EuGH Entscheidung C-184/20, vom 01.08.2022: Ausgangsverfahren u Vorlagefrage*

Durch die oberste litauische Ethikkommission wurde festgestellt, dass der Beschwerdeführer keine, wie oben beschriebene, Erklärung abgegeben habe. Gegen diese Entscheidung ging der Beschwerdeführer gerichtlich vor. Zum einen brachte er vor, dass er nicht zu dem Kreis an Personen gehören würde, welche eine entsprechende Erklärung abgeben müssten. Zum anderen argumentierte er, dass durch die Abgabe einer solchen Erklärung sein Recht auf Achtung des Privatlebens verletzt werden würde. Selbiges würde für andere Personen gelten, zu welchen der Beschwerdeführer gegebenenfalls Erklärungen abgeben müsste. Im weiteren nationalen Verfahren brachte die Oberste Ethikkommission vor, dass die Veröffentlichung der Erklärung zwar ein Eingriff in das Privatleben der betroffenen Personen sei, dieser Eingriff sei jedoch im Gesetz über den Interessenausgleich vorgesehen. Seitens des vorlegenden Gerichts wurde ausgeführt, dass es zweifelhaft sei, ob das Gesetz über den Interessenausgleich bzw die einschlägigen Bestimmungen im Einklang mit den Bestimmungen Art 6 Abs 1 lit c und e und Abs 3 der DSGVO sowie mit Art 9 Abs 1 DSGVO stehen. Die anzugebenden Daten könnten auch besonders sensible Informationen offenlegen, wie beispielsweise, dass die betroffene Person in einer „eheähnlichen Lebensgemeinschaft“ mit einer Person des gleichen Geschlechts lebe. Diese Informationen würden das Potential beinhalten, zu erheblichen „Unannehmlichkeiten“ der Personen zu führen.¹³⁰ Die Informationen würden zudem die persönlichen Beziehungen der erklärungspflichtigen Personen offenbaren. Kritisch angemerkt wurde seitens des vorlegenden Gerichts zusätzlich, dass es für die Erreichung der Ziele des Gesetzes über den Interessenausgleich nicht notwendig wäre, die erhaltenen Informationen über das Internet zu veröffentlichen. Bereits durch die Übermittlung der Erklärung an die Oberste Ethikkommission sowie die Kontrolle und Prüfung durch diese, sei es möglich, die Ziele des Gesetzes, unter anderem Transparenz und die Verwirklichung des öffentlichen Interesses, zu erreichen.¹³¹

In der Folge setzte das Gericht das Verfahren aus und stellte zwei Vorlagefragen an den EuGH. Da sich meines Erachtens wichtige Erkenntnisse, für die in dieser Arbeit thematisierte Problematik, insbesondere aus der zweiten Vorlagefrage ergeben, wird auf die Wiedergabe sowie die Ausführungen zur ersten Vorlagefrage im Wesentlichen verzichtet. Die zweite Vorlagefrage wurde seitens des EuGH folgendermaßen formuliert: *„Mit seiner zweiten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 8 Abs. 1 der Richtlinie 95/46 und Art. 9 Abs. 1 der DSGVO dahin auszulegen sind, dass die Veröffentlichung personenbezogener Daten, die geeignet sind, die*

¹³⁰ Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 36f.

¹³¹ Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 42f.

*politischen Meinungen, die Gewerkschaftszugehörigkeit oder die sexuelle Orientierung einer natürlichen Person indirekt zu offenbaren, auf der Website der Behörde, die für die Entgegennahme und die inhaltliche Kontrolle von Erklärungen über private Interessen zuständig ist, eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne dieser Bestimmungen darstellt.*¹³²

4.2.2.3 EuGH Entscheidung C-184/20, vom 01.08.2022: Entscheidung

Der EuGH führt in seiner Entscheidung aus, dass das vorlegende Gericht es für möglich halten würde, dass aus dem Namen des Ehegatten, welcher veröffentlicht werden müsste, Informationen über die sexuelle Orientierung bzw das Sexualleben abgeleitet werden könnten. Daher sei zu prüfen, ob Daten unter die besonderen Kategorien personenbezogener Daten gemäß Art 9 Abs 1 DSGVO fallen, wenn mittels „gedanklicher Kombination oder Ableitung“ auf die sexuelle Orientierung einer natürlichen Person geschlossen werden kann, auch wenn die Daten „ihrer Natur nach“ keine sensiblen Daten seien.¹³³ Als wichtigen Aspekt für die Auslegung der unionsrechtlichen Vorschriften, führt der EuGH, neben dem reinen Wortlaut der Normen, auch den Kontext und die Ziele der Regelungen an. Weiters wird der Wortlaut des Art 9 Abs 1 DSGVO analysiert und auf das Wort „hervorgehen“ eingegangen.

In den Schlussanträgen des Generalanwalts wurde ausgeführt, dass gemäß Art 9 Abs 1 DSGVO, je nach Art der betroffenen Daten, zwischen drei verschiedenen Verarbeitungen unterschieden werden würde. Als erste Variante wird die Verarbeitung von personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit „hervorgehen“ genannt. Als zweites wird die Verarbeitung genetischer Daten und biometrischer Daten „zur“ eindeutigen Identifizierung einer natürlichen Person genannt. Als letzter Typus wird die Verarbeitung von „Gesundheitsdaten“ oder „Daten zum“ Sexualleben oder der sexuellen Orientierung einer natürlichen Person beschrieben.¹³⁴ Weiters wurde interpretiert, dass sich aus dem Verb „hervorgehen“ ableiten lässt, dass sich die sensible Information nicht direkt aus den vorhandenen Daten ergeben müsste, sondern diese auch indirekt durch den Denkvorgang der „Ableitung oder des Abgleichs“ hergeleitet werden können. Bei der dritten genannten Kategorie (ua Daten zur sexuellen Orientierung) wäre dies jedoch, aufgrund des Wortlautes, nicht möglich. Des Weiteren führt der Generalanwalt aus, dass dies den Schluss zulassen würde, dass die Definition der Verarbeitung von sensiblen Daten abweichen würde, je nach der Art der jeweiligen sensiblen Daten. Eine solche Definition sei seitens des Generalanwalts nicht „wünschenswert“.¹³⁵

¹³² Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 117.

¹³³ Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 119f.

¹³⁴ Siehe GA PIKAMÄE 09.12.2021, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 85.

¹³⁵ Siehe GA PIKAMÄE 09.12.2021, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 85.

Dieser Auslegung widersprach der EuGH. Eine solche Unterscheidung, je nach Art der sensiblen Daten, stehe nicht im Einklang mit der „kontextbezogenen Analyse“ der betroffenen Norm. Eine solche Auslegung würde beispielsweise im Widerspruch zur Definition von Gesundheitsdaten gemäß Art 4 Z15 DSGVO stehen. In dieser Begriffsbestimmung heißt es: *„Gesundheitsdaten‘ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.“*¹³⁶ Auch unter Erwägungsgrund 35 der DSGVO würde für Gesundheitsdaten das Verb „hervorgehen“ verwendet werden.¹³⁷ Meines Erachtens soll durch diesen Verweis darauf hingewiesen werden, dass Gesundheitsdaten in den dritten Typus – wie durch den Generalanwalt beschrieben – von sensiblen Daten fallen würde, da in Art 9 Abs 1 DSGVO nicht unmittelbar das Verb „hervorgehen“ verwendet wird. Daraus würde sich ein Widerspruch innerhalb der DSGVO ergeben, wenn man aus der Formulierung des Art 9 Abs 1 DSGVO eine solche Typisierung ableitet.

Zusätzlich zu diesen Argumenten führt der EuGH an, dass sich eine weite Auslegung des Begriffs der „besonderen Kategorien personenbezogener Daten“ aus den Zielen der DSGVO (sowie seiner Vorgängerbestimmung) ergeben würde, welche vorsehen ein möglichst hohes Schutzniveau zu schaffen. Des Weiteren sei insbesondere der Zweck des Art 9 Abs 1 DSGVO, dass ein vor allem erhöhter Schutz der Datenverarbeitung gewährleistet wird. Dies wäre insbesondere aufgrund der besonderen Sensibilität der betreffenden Daten und einer daraus resultierenden schwere eines Eingriffs erforderlich.¹³⁸ Daraus schlussfolgert der EuGH, dass von dem besonderen Schutz des Art 9 Abs 1 DSGVO auch solche Verarbeitungen von personenbezogenen Daten erfasst sein sollen, die indirekt sensible Daten über eine natürliche Person offenbaren können.

Daher entschied der EuGH die Vorlagefrage wie folgt: *„Nach alledem ist auf die zweite Frage zu antworten, dass Art. 8 Abs. 1 der Richtlinie 95/46 und Art. 9 Abs. 1 der DSGVO dahin auszulegen sind, dass die Veröffentlichung personenbezogener Daten, die geeignet sind, die sexuelle Orientierung einer natürlichen Person indirekt zu offenbaren, auf der Website der Behörde, die für die Entgegennahme und die inhaltliche Kontrolle von Erklärungen über private Interessen zuständig ist, eine Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne dieser Bestimmungen darstellt.“*¹³⁹

¹³⁶ Siehe Art 4 Z 15 DSGVO.

¹³⁷ Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 124.

¹³⁸ Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 125f.

¹³⁹ Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 128.

4.2.3 Literaturresonanz zu EuGH Entscheidung C-184/20, vom 01.08.2022

Die zuvor beschriebene Entscheidung führte auch in der Literatur zu einer gewissen Resonanz. In der Folge wird daher aufgezeigt, wie die Entscheidung Einfluss auf die bisherigen Standpunkte in der Lehre nimmt.

Mit der gegenständlichen Entscheidung des EuGH führt dieser im Wesentlichen seine, den Schutz von Betroffenen stärkende, Auslegung der DSGVO fort. Wie sich bereits in der Entscheidung *Lindquist* ergab, wird von einer weiten Auslegung des Begriffs der besonderen Kategorien personenbezogener Daten ausgegangen.¹⁴⁰ Wichtig ist zudem anzumerken, dass sich die Entscheidung zwar auf ein Verfahren bezieht, in welchem die Ableitung von Informationen über das Sexualleben einer natürlichen Person fraglich war, der EuGH jedoch an einigen Stellen allgemein Bezug auf die Auslegung von sensiblen Daten im Sinne der DSGVO nimmt.¹⁴¹ Da für die Verarbeitung von Lichtbildern keine eigenen Regeln im Regime der DSGVO gelten, lassen sich die gewonnen Erkenntnisse auch auf solche Verarbeitungen übertragen. *Laimighofer* sieht die Nähe von optischen Merkmalen zu sensiblen Daten, welche sich daraus ableiten lassen, sogar tendenziell als größer an als in der Ableitbarkeit der sexuellen Orientierung einer Person aufgrund des Namens des Partners.¹⁴² Demzufolge sollten sich die Erkenntnisse dieser Entscheidung auch auf Lichtbildaufnahmen übertragen lassen.

Als wesentliche Erkenntnis der gegenständlichen Entscheidung kann genannt werden, dass auch die Verarbeitung solcher Informationen, aus denen sich indirekt, mittels „gedanklicher Kombination“, sensible Daten ableiten lassen, dem besonderen Schutz des Art 9 DSGVO unterliegen soll bzw von diesem nicht ausgenommen ist.¹⁴³ Ein solcher Vorgang der „gedanklichen Kombination“ könnte im Zusammenhang mit einer Bildaufnahme darin bestehen, dass ein bestimmtes körperliches Symptom mit einer Krankheit verglichen wird, oder beispielsweise ein bestimmtes Kleidungsstück mit einer religiösen Überzeugung in Verbindung gebracht wird.¹⁴⁴

Als weitere Erkenntnis lässt sich aus dieser Entscheidung ableiten, dass der EuGH wohl eine Unterscheidung zwischen sensiblen Daten „ihrer Natur“ und solcher, welche sich erst aus einer gedanklichen Kombination heraus ergeben, befürwortet.¹⁴⁵ Eine Unterscheidung zwischen diesen beiden „Arten“ sensibler Daten bzw eine scharfe Trennlinie, lässt sich meines Erachtens jedoch nur

¹⁴⁰ Siehe *Gosch*, *jusIT* 2022/76, 183 (185).

¹⁴¹ Vgl auch *Gosch*, *jusIT* 2022/76, 183 (185).

¹⁴² Siehe *Laimighofer*, *jusIT* 2023, 102 (105).

¹⁴³ Vgl *Kienle*, *LTZ* 2023, 50 (66).

¹⁴⁴ Vgl *Laimighofer*, *jusIT* 2023, 102 (105).

¹⁴⁵ Vgl *Kienle*, *LTZ* 2023, 50 (66).

schwierig erkennen. Daher stellt sich nach wie vor die Frage, ob diese (weite) Auslegung des Schutzes des Art 9 Abs 1 DSGVO in irgendeiner Form Spielraum für eine teilweise Begrenzung zulässt.

Darüber hinaus zeigt sich in der Literatur auch Kritik an dieser Entscheidung. Ein solch weites Verständnis von der Verarbeitung von besonderen Kategorien personenbezogener Daten könnte, gemäß *Kienle*, Gefahr laufen, dass der Datenschutz in dieser Hinsicht zu einem absoluten Recht „mutieren“ würde.¹⁴⁶ Möglicherweise hat es der EuGH lediglich verabsäumt bzw nicht als notwendig erachtet, im Zuge der gegenständlichen Entscheidung weiterführende Einschränkungen der Klassifikation von sensiblen Daten vorzunehmen.¹⁴⁷

Unabhängig davon besteht natürlich die Möglichkeit bzw im Sinne des Grundsatzes der Datenminimierung gemäß Art 5 lit c DSGVO auch die Verpflichtung dazu, nur das notwendige Maß an personenbezogenen Daten überhaupt zu erheben. In einem der Verarbeitung der Daten vorgelagerten Schritt wäre es möglich, auszuwerten, ob sich aus den zu erhebenden Informationen auch sensible Daten ableiten lassen können, um eine Verarbeitung dieser bereits im Vorfeld zu verhindern.¹⁴⁸ Da eine solche Umsetzung in der Praxis vermutlich diverse Probleme verursachen könnte (beispielsweise das stetige Hinzutreten von weiteren personenbezogenen Daten, welche an einem gewissen Punkt zu einer Ableitbarkeit sensibler Informationen führen könnten)¹⁴⁹ und die Ausnahmetabestände des Art 9 Abs 2 DSGVO nicht für alle Verarbeitungen praktikabel wären, dürfte der praktische Bedarf an zulässigen Eingrenzungen des Verbots der Verarbeitung von sensiblen Daten vorhanden sein.

Eine gewisse Abgrenzung wäre beispielsweise durch das Heranziehen der jeweiligen Begriffsbestimmungen der einzelnen (besonderen) Kategorien denkbar. Die Definitionen des Art 4 DSGVO geben bereits gewisse Anforderungen vor, welche die Informationen erfüllen müssen, um von den besonderen Kategorien erfasst zu sein.¹⁵⁰ Meines Erachtens vermag dies aber für die Verarbeitung von Lichtbildern von natürlichen Personen kaum eine Eingrenzung zu bieten. Insbesondere Merkmale, welche auf die rassische oder ethnische Herkunft einer Person schließen lassen, könnten unter dieser (weiten) Auslegung des Art 9 Abs 1 DSGVO durchaus aus einem „einfachen“ Lichtbild hervorgehen. Die bloße Beschränkung durch die Definitionen der besonderen Kategorien vermag daran nichts zu ändern.

¹⁴⁶ Siehe *Kienle*, LTZ 2023, 50 (67).

¹⁴⁷ Siehe *Gosch*, jusIT 2022/76, 183 (187).

¹⁴⁸ Siehe *Gosch*, jusIT 2022/76, 183 (188).

¹⁴⁹ Vgl *Gosch*, jusIT 2022/76, 183 (188).

¹⁵⁰ Vgl *Gosch*, jusIT 2022/76, 183 (186); *Jahnel*, DSGVO Art 9 DSGVO Rz 17.

Vor dieser Entscheidung ist für Anwendungsfälle mit Lichtbildern (Videoüberwachung, etc) der Verwendungszweck bzw der Verwendungszusammenhang herangezogen worden, um die Anwendbarkeit des Art 9 DSGVO auszuschließen.¹⁵¹ In der gegenständlichen Entscheidung wurde jedoch nicht der Verwendungszweck bei der Prüfung berücksichtigt. Wie *Gosch* formuliert, könnte im gegenständlichen Urteil die Verarbeitung der Interessenerklärung durch die Oberste Ethikkommission nicht darauf gerichtet sein, dass hierbei die sexuelle Orientierung und damit ein sensibles Datum einer natürlichen Person veröffentlicht werden soll. Versucht doch das Gesetz über den Interessenausgleich sensible Daten von der gesetzlichen Pflicht zur Veröffentlichung auszunehmen. Im Sinne dieser Entscheidung sei es daher abzulehnen, dass die Reichweite des Begriffs der sensiblen Daten durch den Zweck der Verarbeitung begrenzt wird.¹⁵² Auf den (objektiven) Verwendungszusammenhang, wie er beispielsweise auch von *Jahnel* beschrieben wurde,¹⁵³ geht der EuGH ebenso wenig wie auf den Verarbeitungszweck ein. Der Meinung von *Kienle* folgend, werden damit diese beiden Ansätze „unausgesprochen“ durch den EuGH zurückgewiesen.¹⁵⁴ *Gosch* geht bezüglich dieser Auslegung sogar noch einen Schritt weiter und stellt die Argumentation auf, dass der Verarbeitungszweck nicht als Begrenzung der Reichweite des Begriffs der sensiblen Daten herangezogen werden kann, aber als Indikator für das Vorliegen einer Verarbeitung von sensiblen Daten dienen könnte. Würde doch durch den Zweck der Verarbeitung (das Extrahieren von sensiblen Daten) geradezu darauf hingewiesen werden, dass sich aus den entsprechenden Daten sensible Informationen ableiten lassen könnten.¹⁵⁵

Jedenfalls wurde in dieser Entscheidung des EuGH die durch GA Pikamäe vorgebrachte und auch in der Literatur beispielsweise durch *Jahnel* vertretene Auslegung, dass die besonderen Kategorien personenbezogener Daten nach verschiedenen Typen zu kategorisieren seien,¹⁵⁶ nicht bestätigt.¹⁵⁷ Diese Auslegung des EuGH deckt sich nicht mit jener, insbesondere im deutschsprachigen Raum vertretenen, Interpretation des Art 9 Abs 1 DSGVO und dem Verständnis des Wortes „hervorgehen“.¹⁵⁸ Schlussendlich sind die „verschiedenen Kategorien“ daher einheitlich zu beurteilen und im gleichen Sinne weit auszulegen. Die gegenständliche Entscheidung unterstützt daher am ehesten eine objektive Auslegung, wie sie etwa von *Bergauer* formuliert wurde. Dieser formulierte

¹⁵¹ Vgl *Hense*, KuR 2023, 556 (559).

¹⁵² Siehe *Gosch*, *jusIT* 2022/76, 183 (186f).

¹⁵³ Siehe *Jahnel*, DSGVO Art 9 DSGVO Rz 20.

¹⁵⁴ Siehe *Kienle*, LTZ 2023, 50 (67).

¹⁵⁵ Siehe *Gosch*, *jusIT* 2022/76, 183 (187).

¹⁵⁶ Vgl auch *Schiff* in DS-GVO² Art 9 DSGVO Rz 13; *Frenzel* in DS-GVO BDSG³ Art 9 DSGVO Rz 8.

¹⁵⁷ Siehe EuGH 01.08.2022, C-184/20 (*Vyriausioji tarnybinės etikos komisija*) Rz 124ff; vgl auch *Gabauer*, *Weite Auslegung der Begriffe „besondere Kategorien personenbezogener Daten“ und „sensible Daten“*, RdM-LS 2023/63, 115.

¹⁵⁸ Siehe *Kastelitz/Hötzendorfer/Tschohl* in *DatKomm* Art 9 DSGVO Rz 19; *Schiff* in DS-GVO² Art 9 DSGVO Rz 13; *Frenzel* in DS-GVO BDSG³ Art 9 DSGVO Rz 8.

bereits 2016, dass eine objektive Betrachtung geboten sei, um das hohe Schutzniveau der DSGVO nicht aufzuweichen und das erhöhte Risiko, welches aus der Verarbeitung von sensiblen Daten hervorgeht, anhand einer „objektiven Bewertung“ zu beurteilen sei.¹⁵⁹

Da eine solch weite objektive Auslegung, wie sie aus dem gegenständlichen Urteil abzuleiten ist, dazu führen könnte, dass bereits jede theoretisch mögliche Ableitung von sensiblen Informationen zu einer Anwendung des Art 9 DSGVO führen könnte, ist in der Folge zu prüfen, ob die teleologische Reduktion der „hinlänglichen Sicherheit“, wie sie beispielsweise von *Bergauer* formuliert wurde, zu einer gewissen Eingrenzung des Anwendungsbereichs des Art 9 DSGVO führen kann.¹⁶⁰

Der Ansicht von *Gosch* folgend, könnte durch das Abstellen auf ein solches Kriterium in gewissen Konstellationen der Schutzzadius für die Verarbeitung von personenbezogenen Daten stark eingeschränkt werden.¹⁶¹ Im gegenständlichen Urteil des EuGH wäre dieser, ihrer Auffassung nach, zu einem anderen Ergebnis gekommen, hätte er das Kriterium der „hinlänglichen Sicherheit“ auf den betroffenen Sachverhalt angewendet. Das Bestehen einer Ehe oder Lebenspartnerschaft reiche nicht aus, um mit „hinlänglicher Sicherheit“ auf die Sexualität einer Person schließen zu können. Zu dieser Erkenntnis gelangt *Gosch* aufgrund der Vielzahl an verschiedenen Beziehungsmodellen, welche auch im Rahmen einer Ehe bzw eingetragenen Partnerschaft bestehen können (Asexualität, Scheinehen, etc). Der EuGH habe bei seiner Entscheidung nur auf die Eignung der personenbezogenen Daten abgestellt, indirekt die sexuelle Orientierung einer Person zu offenbaren.¹⁶²

Eine etwas weiter relativierende Ansicht vertritt in diesem Zusammenhang beispielsweise *Deiters*. Zwar gebe es in der Realität durchaus „Zweckehen“ oder ähnliche Konstruktionen, welche entgegen der sexuellen Orientierung zu verstehen sind, jedoch habe man in diesem konkreten Fall von Daten ausgehen können, welche Rückschlüsse auf die sexuelle Orientierung zulassen würden. Bei der Information, dass eine Person mit einer anderen Person des gleichen Geschlechts verheiratet sei, ließe sich auf ein solches sensibles Kriterium abstellen, bzw würde diese Information offenbart, auch ohne, dass die konkrete „Hingezogenheit“ zu diesem Geschlecht ausdrücklich erfolgen würde.¹⁶³

Als begrenzendes Kriterium vertritt *Deiters* die Ansicht, dass in Fällen einer „indirekten Offenlegung“ nur solche Verarbeitungen unter den Bestimmungen des Art 9 DSGVO zu beurteilen sind, aus welchen sich „zwingende Rückschlüsse“ auf sensible Daten ableiten lassen. In anderen Worten, die

¹⁵⁹ Siehe *Bergauer*, *jusIT* 2016/103, 241 (245f).

¹⁶⁰ Vgl *Bergauer*, *jusIT* 2016/103, 241 (246).

¹⁶¹ Siehe *Gosch*, *jusIT* 2022/76, 183 (187).

¹⁶² Siehe *Gosch*, *jusIT* 2022/76, 183 (187).

¹⁶³ Siehe *Deiters*, EuGH zu Art. 9 Abs. 1 DSGVO: Sind nun „alle“ Daten besondere Kategorien personenbezogener Daten?, *DSB* 2022, 247 (248).

Rückschlüsse sollten sich (weitestgehend) zwingend ergeben.¹⁶⁴ Eine solche Abgrenzung würde seiner Ansicht nach dazu führen, dass beispielsweise durch das Bestellen eines Medikaments in einer Online-Apotheke oder das Kaufen bestimmter Lebensmittel kein entsprechend „zwingender“ Rückschluss auf beispielsweise Gesundheitsdaten möglich wäre. Auch wenn häufig aus diesen Informationen auf ein entsprechendes Gesundheitsdatum rückgeschlossen werden könnte, seien die Informationen nicht ausreichend. Schließlich bestünde auch die Möglichkeit, dass der Besteller lediglich für einen Angehörigen entsprechende Produkte erwerben würde.¹⁶⁵ Diese Interpretationsweise kann meines Erachtens in ein ähnliches Spektrum wie das von *Bergauer* definierte Kriterium der „hinlänglichen Sicherheit“ eingestuft werden.

Laimighofer vertritt entgegen diesen Überlegungen die Ansicht, dass der EuGH auch bei Berücksichtigung des Kriteriums der „hinlänglichen Sicherheit“ zu einem identen Ergebnis in der gegenständlichen Entscheidung gekommen wäre. Es würde der allgemeinen Lebenserfahrung entsprechen, dass das Geschlecht des jeweiligen Partners mit der sexuellen Orientierung einer Person zusammenhängt. Unter der Voraussetzung, dass man an das Kriterium der „hinlänglichen Sicherheit“ keinen übertrieben strengen Maßstab ansetzt, sei auch in dem gegenständlichen Fall das Kriterium erfüllt. Das Kriterium erfordere keine hundertprozentige Gewissheit. Wie bereits unter Punkt 4.1.2 ausgeführt, würde das Wort „hervorgehen“ – auf welches der EuGH in dem gegenständlichen Urteil genauer eingeht – bereits eine ähnliche Funktion erfüllen. Dem Kriterium der „hinlänglichen Sicherheit“ würde in diesem Zusammenhang kein Mehrwert zukommen, weshalb der EuGH nicht nach diesem Kriterium prüfen würde.¹⁶⁶

Mit der Frage, wie sich die Erkenntnisse aus der EuGH Entscheidung C-184/20 vom 01.08.2022 auf Bilddateien anwenden lassen, hat sich insbesondere *Laimighofer* auseinandergesetzt. Seiner Ansicht folgend, müsste an erster Stelle eine Bildaufnahme einer real existierenden Person zugeordnet (Identifiziert) werden können. Andernfalls würde es sich lediglich um das Lichtbild eines Menschen handeln, auf dem unter Umständen auch Informationen, wie beispielsweise die Ethnie oder die religiöse Überzeugung enthalten sind. Diese Informationen müssten aber einer konkreten Person zugeordnet sein.¹⁶⁷ Diese Identifizierung könne beispielsweise anhand von biometrischen Daten erfolgen. Allerdings ist hervorzuheben, dass auch jede andere Zuordnung einer Bildaufnahme zu einer natürlichen Person dazu führen könne, dass das auf einem Bild „ersichtliche sensible Merkmal“ zu einer der besonderen Kategorien von personenbezogenen Daten werden könne.¹⁶⁸ Hierbei käme

¹⁶⁴ Siehe *Deiters*, DSB 2022, 247 (249).

¹⁶⁵ Siehe *Deiters*, DSB 2022, 247 (249).

¹⁶⁶ Siehe *Laimighofer*, *jusIT* 2023, 102 (106).

¹⁶⁷ Siehe *Laimighofer*, *jusIT* 2023, 102 (105).

¹⁶⁸ Siehe *Laimighofer*, *jusIT* 2023, 102 (105).

es weiters nicht auf den Zweck der Datenverarbeitung an. So würde beispielsweise ein Unternehmen, welches Bilder der Mitarbeiter:innen auf der eigenen Website online veröffentlicht, in der Regel nicht den Zweck verfolgen, sensible Daten seiner Beschäftigten (wie beispielsweise die Ethnie) zu verarbeiten. Dadurch, dass die Informationen aber einer bestimmten Person zugeordnet werden könne, könnten die Daten – in einer solchen Konstellation – sensible Daten darstellen.¹⁶⁹

Weiter argumentiert *Laimighofer*, dass bei diesen Überlegungen kein Widerspruch zur ständigen Judikatur bestehen würde. Diese geht davon aus, dass Personenbezug auch in den Konstellationen besteht, in denen Bildaufnahmen beispielsweise mittels einer Überwachungskamera von einer Person aufgenommen wurden, auch wenn diese Bilder nicht unmittelbar die Identifikation der entsprechenden Person ermöglichen. Für die Erfüllung der Eigenschaft des „personenbezogenen Datums“ sei es nicht erforderlich, dass die Daten ohne ergänzende Informationen unmittelbar einer natürlichen Person zugeordnet werden können. Ausreichend sei es, dass die abgelichtete Person bestimmbar sei. Für Bildaufnahmen sei es daher erforderlich, dass diese die Identifikation der entsprechenden Person ermöglichen. Hierzu verweist *Laimighofer* auf die Judikatur des EuGH betreffend des Vorliegens der Eigenschaft des „personenbezogenen Datums“ von dynamischen IP Adressen.¹⁷⁰ Aus dieser Entscheidung geht unter anderem hervor, dass dynamische IP Adressen für einen Anbieter von Online-Mediendiensten personenbezogene Daten im Sinne der Datenschutz-RL, darstellen, wenn dieser Anbieter über rechtliche Mittel verfügt, die betreffende Person mittels Zusatzinformationen, welche dem Internetzugangsanbieter zur Verfügung stehen, zu bestimmen.¹⁷¹

In einem nächsten Schritt unterscheidet *Laimighofer* zwischen dem „Personenbezug“ des Begriffs „personenbezogenen Daten“ sowie der Verbindung, welche zwischen einer sensiblen Information und einer natürlichen Person gefordert wird, damit das Kriterium des „Hervorgehens“ im Sinne des Art 9 Abs 1 DSGVO erfüllt wird. Der Unterschied solle demnach darin liegen, dass der Begriff des „Hervorgehens“ voraussetzt, dass die sensiblen Informationen mit der entsprechenden Person bereits aufgrund der jeweiligen Daten in Verbindung gebracht werden könne. Für biometrische Daten, wie sie in Erwägungsgrund 51 beschrieben werden, sei dieses Kriterium gegeben. Als Beispiel für andere Konstellationen, in denen diese beschriebene Verbindung zwischen sensiblem Datum und einer Person gegeben sei, wird angeführt, wenn der Name der betroffenen Person mit der sensiblen Information gemeinsam verarbeitet werden würde, oder andere Informationen der Person zugewiesen seien, aus denen mittelbar oder unmittelbar ermöglicht werden würde, dass die sensible

¹⁶⁹ Siehe *Laimighofer*, *jusIT* 2023, 102 (105).

¹⁷⁰ Siehe *Laimighofer*, *jusIT* 2023, 102 (104f); EuGH 19.10.2016, C-582/14 (Breyer).

¹⁷¹ Siehe EuGH 19.10.2016, C-582/14 (Breyer) Rz 49; *Jahnel*, EuGH: Dynamische IP-Adressen sind personenbezogene Daten, *jusIT* 2016/105, 252 (252f).

Information der betroffenen Person zugeordnet wird. Wichtig sei hierbei, dass die Zuordnung der sensiblen Information allein aufgrund der bereits vorliegenden Daten möglich sein müsste.¹⁷²

Diese zuvor beschriebene Unterscheidung hätte zur Folge, dass insbesondere Daten, welche pseudonymisiert wären, nach wie vor als personenbezogenen Datum anzusehen seien. Durch die Pseudonymisierung sei die sensible Information jedoch nicht mehr einer bestimmten Person zuordenbar, das Kriterium der Identifizierbarkeit würde daher diesen Datensätzen fehlen. Für das Ableiten der sensiblen Informationen ist es daher erforderlich, dass die jeweilige Person auch Zugriff auf die Entschlüsselung der Pseudonymisierung haben müsste. Nur durch die Entschlüsselung wäre es möglich, dass die Zuordnung der sensiblen Informationen zu einer bestimmten Person erfolgen könnte. Zugriff auf die sensiblen Daten hätten daher nur jene Personen, welche auch Zugriff auf die nicht-pseudonymisierten Datensätze hätten.¹⁷³ Eine unmittelbare Zuordnung würde jedoch seitens des EuGHs für das Vorliegen eines „Hervorgehens“ nicht verlangt werden. Daher könne ab dem Zeitpunkt von einem indirekten Hervorgehen von sensiblen Informationen gesprochen werden, sobald sowohl Zugriff auf den pseudonymisierten Datensatz als auch auf den entsprechenden „Pseudonymisierungs-Schlüssel“ bestehen würde.¹⁷⁴ Diesen Überlegungen folgend, könnte daher die Problematik der (ungewünschten Mit-) Verarbeitung von sensiblen Daten zumindest in den Fällen abgewendet werden, in denen eine Pseudonymisierung von Datensätzen möglich ist. In Frage gestellt wird hierbei nicht, dass es sich bei der Verarbeitung der Datensätze, auch wenn der Zugriff auf die jeweilige Entschlüsselung nicht besteht, nach wie vor um die Verarbeitung von personenbezogenen Daten handelt und daher die entsprechenden Anforderungen der DSGVO diesbezüglich eingehalten werden müssten.

4.2.3.1 Exkurs: EuG T-557/20 vom 26.04.2023

In diesem Zusammenhang kann auf eine jüngere Entscheidung des EuG vom 26.04.2023 verwiesen werden.¹⁷⁵ In dieser Entscheidung beschäftigte sich das EuG unter anderem mit der Frage, ob Personenbezug auch bei solchen Datensätzen angenommen werden könnte, bei denen eine Pseudonymisierung vorliegen würde und ein Dritter, welcher keinen Zugriff auf die entsprechenden Entschlüsselungen hätte, diese Daten verarbeitet. Das EuG verweist in seiner Entscheidung auf die Rechtsprechung des EuGH in der Rechtssache „Breyer“ aus dem Jahr 2016¹⁷⁶ und spricht sich wohl für ein relatives Verständnis des Personenbezugs aus. Der EDSB hatte es im Ausgangsverfahren unterlassen zu prüfen, ob die verarbeiteten Informationen für den entsprechenden Empfänger

¹⁷² Siehe *Laimighofer*, *jusIT* 2023, 102 (106).

¹⁷³ Siehe *Laimighofer*, *jusIT* 2023, 102 (107).

¹⁷⁴ Siehe *Laimighofer*, *jusIT* 2023, 102 (107).

¹⁷⁵ Siehe EuG 26.04.2023, T-557/20.

¹⁷⁶ Siehe EuGH 19. 10. 2016, C-582/14 (Breyer).

„personenbeziehbar“ seien.¹⁷⁷ Für die Annahme, dass es sich um personenbezogene Daten handeln würde, reichte es für den EDSB aus, dass zusätzliche Informationen zur Rückidentifizierung grundsätzlich existieren würden.¹⁷⁸ Der EDSB hätte jedoch prüfen müssen, ob aus Sicht des Empfängers das Recht besteht, auf diese Entschlüsselungsdaten zuzugreifen und ob dieser Zugriff „praktisch durchführbar“ gewesen wäre.¹⁷⁹ Diese Entscheidung könnte insbesondere für die oben geschilderten Überlegungen von *Laimighofer* relevant sein, da durch einen möglichen Ausschluss des Personenbezugs, im Falle einer entsprechenden Pseudonymisierung, jedenfalls auch keine Verarbeitung von sensiblen Daten erfolgen würde.

Bisher wurde in der Literatur beispielsweise von *Gosch* und *Kastelitz/Hötzendorfer/Tschohl* die Ansicht vertreten, dass die Pseudonymisierung nichts an der Einstufung von Daten als sensible Daten ändern würde. Die Pseudonymisierung habe dieser Ansicht folgenden keinen Einfluss auf die Sensibilität der Daten.¹⁸⁰ Der Vollständigkeit halber wird jedoch darauf hingewiesen, dass in dem gegenständlichen Verfahren vor dem EuG die EU-DSVO¹⁸¹ und nicht die DSGVO zur Anwendung kam (auch wenn die für diese Entscheidung relevanten Normen der EU-DSVO den Bestimmungen der DSGVO im Wesentlichen nachgebildet sind).¹⁸² Es bleibt daher abzuwarten, ob der EuGH die Entscheidung des EuG bestätigen wird.

4.2.4 Judikatur: EuGH Entscheidung C-252/21, vom 04.06.2023

Der gegenständlichen Entscheidung liegt ein Sachverhalt zugrunde, welcher sich in erster Linie auf die Kompetenzen der nationalen Wettbewerbsbehörden bezieht. In der weiteren Folge werden jedoch auch Vorlagefragen an den EuGH gestellt, welche sich auf die Zulässigkeit der Verarbeitung von personenbezogenen Daten beziehen. Daher soll auch diese EuGH-Entscheidung nachstehend genauer betrachtet werden.

4.2.4.1 EuGH Entscheidung C-252/21, vom 04.06.2023: Ausgangsverfahren u Vorlagefrage

Der Hintergrund der oben genannten Entscheidung ist ein Beschwerdeverfahren, welches durch Meta (vormals Facebook) gegen das deutsche Bundeskartellamt geführt wurde.¹⁸³ Das deutsche Bundeskartellamt hatte 2019 mittels Beschluss mehreren Gesellschaften des Meta-Konzerns im

¹⁷⁷ Siehe *Baumgartner*, Bestimmung des Personenbezugs von Daten, ZD 2023, 399 (403).

¹⁷⁸ Siehe EuG 26.04.2023, T-557/20 Rz 101ff.

¹⁷⁹ Siehe EuG 26.04.2023, T-557/20 Rz 105ff.

¹⁸⁰ Siehe *Gosch*, Pseudonymisierung und Verschlüsselung sensibler Daten, jusIT 2019/39, 107 (110); *Kastelitz/Hötzendorfer/Tschohl* in *DatKomm* Art 9 DSGVO Rz 19.

¹⁸¹ Siehe Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABI L 2018, 295/39, in der Folge kurz „EU-DSVO“.

¹⁸² Vgl. *Thiele*, EuG: Zum relativen Personenbezug von Daten, jusIT 2023/65, 151 (152).

¹⁸³ Siehe auch *Hense*, KuR 2023, 556 (557).

Wesentlichen untersagt, dass diese in ihren Allgemeinen Nutzungsbedingungen die Nutzung des sozialen Netzwerks Facebook von der Zustimmung des Nutzers abhängig machten, dass auch sogenannte Off-Facebook-Daten (über diese Daten können die Nutzungsaktivitäten auch abseits von Facebook analysiert werden) verarbeitet werden können. Für die Verarbeitung bzw die Erhebung der Off-Facebook-Daten verwendete Meta unter anderem Cookies.¹⁸⁴ Relevant waren in diesem Zusammenhang die Verarbeitung von privaten Nutzerdaten von Personen, welche in Deutschland wohnhaft waren. Begründet wurde der Beschluss damit, dass Facebook seine markbeherrschende Stellung ausgenutzt habe, um die entsprechenden AGB auf die Nutzer anwenden zu können. Problematisch seien die AGB insbesondere, da die genannte Verarbeitung nicht mit den Werten der DSGVO im Einklang stünden und dieser Verarbeitung insbesondere nicht gemäß Art 6 Abs 1 sowie Art 9 Abs 2 DSGVO gerechtfertigt werden könnte.¹⁸⁵ Durch die betroffenen Meta-Gesellschaften wurde Beschwerde beim OLG Düsseldorf eingebracht. Dieses zweifelte unter anderem daran, ob eine nationalen Wettbewerbsbehörde befugt sei, die Erfüllung der Anforderungen der DSGVO zu prüfen. Des Weiteren zweifelte das OLG Düsseldorf, neben anderen Punkten daran, ob es für Betreiber von sozialen Netzwerken zulässig sei, sensible Daten im Sinne des Art 9 DSGVO zu verarbeiten.¹⁸⁶

Für die gegenständliche Arbeit ist insbesondere der erste Teil der zweiten Vorlagefrage relevant, weshalb auf die Thematisierung der anderen Fragen an dieser Stelle verzichtet wird. Die zweite Vorlagefrage (lit a) des OLG Düsseldorf lautet wie folgt:

„Handelt es sich dann, wenn ein Internetnutzer Webseiten oder Apps, die Bezug zu den Kriterien des Art. 9 Abs. 1 DSGVO haben, wie etwa Flirting-Apps, Homosexuellen-Partnerbörsen, Webseiten politischer Parteien, gesundheitsbezogene Webseiten, entweder nur aufruft oder dort auch Eingaben tätigt, etwa bei Registrierung oder Bestellungen, und ein ... Unternehmen wie Meta Platforms Ireland über in die Webseiten und Apps eingebundene Schnittstellen, wie „Facebook Business Tools“, oder über auf dem Computer oder mobilen Endgerät des Internetnutzers eingesetzte Cookies oder ähnliche Speichertechnologien die Daten über den Aufruf der Webseiten und Apps durch den Nutzer und über dort getätigte Eingaben des Nutzers erfasst, mit den Daten des Facebook.com-Kontos des Nutzers verknüpft und verwendet, bei der Erfassung und/oder der Verknüpfung und/oder der Verwendung um die Verarbeitung sensibler Daten im Sinne der Norm?“¹⁸⁷

¹⁸⁴ Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 28ff.

¹⁸⁵ Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 30.

¹⁸⁶ Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 34.

¹⁸⁷ Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 35.

4.2.4.2 EuGH Entscheidung C-252/21, vom 04.06.2023: Entscheidung

Der EuGH sprach im Wesentlichen aus, dass eine solche Verarbeitung (ua Verknüpfung und Sammlung der Off-Facebook-Daten) von personenbezogenen Daten eine Verarbeitung von sensiblen Daten darstellen kann, wenn hierdurch die Offenlegung von Informationen ermöglicht wird, die unter die besonderen Kategorien des Art 9 Abs 1 DSGVO fallen.

Hense beschreibt die Prüfung des EuGH von Art 9 Abs 1 DSGVO in Verbindung mit Erwägungsgrund 51 als lehrbuchhaft.¹⁸⁸ Das Höchstgericht verweist in seiner Entscheidung auf die erheblichen Risiken, welche aus der Verarbeitung von sensiblen Daten entstehen können und den Grundsatz, dass gemäß Art 9 Abs 1 DSGVO eine Verarbeitung solcher Daten daher grundsätzlich untersagt ist. Daher sei relevant, ob aus der Verarbeitung der Daten durch Meta, auch eine Offenlegung von Informationen ermöglicht wird, die in die besonderen Kategorien von personenbezogenen Daten „fallen“.¹⁸⁹ Bereits in den Schlussanträgen zu dieser Entscheidung brachte der Generalanwalt vor, dass es bei der Einstufung von Daten als sensible Daten nicht auf den Wahrheitsgehalt, also die Richtigkeit der Einstufung unter eine der Kategorien des Art 9 Abs 1 DSGVO, ankäme. Darüber hinaus sei auch nicht das Ziel einer Verarbeitung entscheidend für die Kategorisierung als sensible Daten.¹⁹⁰ Dieser Ansicht folgend, sei das Ziel der entsprechenden Bestimmung im Wesentlichen *„[...] in objektiver Weise erheblichen Gefahren für die Grundrechte und Grundfreiheiten der betroffenen Personen vorzubeugen, die sich aus der Verarbeitung sensibler personenbezogener Daten ergeben, unabhängig von jedem subjektiven Element wie der Absicht des für die Verarbeitung Verantwortlichen.“*¹⁹¹ An dieser Auslegung orientierte sich auch der EuGH. Das grundsätzliche Verarbeitungsverbot von sensiblen Daten gilt unabhängig davon, ob der Verantwortliche mit dem Ziel handelt, Informationen zu erlangen, welche unter eine der Kategorien von sensiblen Daten fallen und ob durch die entsprechende Information, die durch die Verarbeitung offengelegt wird, der Wahrheit entspricht.¹⁹² Weiters würde die Bestimmung des Art 9 Abs 1 DSGVO, unabhängig von dem erklärten Zweck, Datenverarbeitungen, aufgrund der Risiken für die Grundrechte und Grundfreiheiten von betroffenen Personen, verbieten.¹⁹³ Ob in dem der Entscheidung zugrundeliegenden Verfahren tatsächlich die Offenlegung von solchen Informationen ermöglicht werden würde, überließ der EuGH dem vorlegenden Gericht zu prüfen.¹⁹⁴

¹⁸⁸ Siehe Hense, KuR 2023, 556 (559).

¹⁸⁹ Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 66-68.

¹⁹⁰ Siehe GA RANTOS 20.09.2022, C-252/21 Rz 40.

¹⁹¹ Siehe GA RANTOS 20.09.2022, C-252/21 Rz 41.

¹⁹² Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 69.

¹⁹³ Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 70.

¹⁹⁴ Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 71.

4.2.5 Literaturresonanz zu EuGH Entscheidung C-252/21, vom 04.06.2023

Durch die soeben beschriebene Entscheidung wird die Judikatur-Linie, welche der EuGH bereits in seiner Entscheidung C-184/20, vom 01.08.2022, angedeutet hat, weiter verstärkt. Auch diese Entscheidung geht von einer sehr weiten Auslegung des Schutzes durch Art 9 Abs 1 DSGVO aus und legt die entsprechenden Normen in sehr grundrechtsfreundlicher Weise aus.¹⁹⁵ Allerdings wurde der EuGH in vergangenen Entscheidungen nicht so eindeutig, wie er es in seinem gegenständlichen Urteil wurde. In der Literatur wird die Ansicht vertreten, dass der EuGH mit dieser Entscheidung eine klare Absage den Überlegungen erteilt hat, welche die Anwendung des besonderen Schutzes von sensiblen Daten von der subjektiven Zweckbestimmung oder der Absicht der Auswertung abhängig machen wollten.¹⁹⁶ Gemäß *Hense* würde die Datenverarbeitung, insbesondere auch in Bereichen wie Scoring oder Machine-Learning, von dieser Entscheidung weit beeinflusst werden und könnte dazu führen, dass die entsprechenden Verarbeitungen bisher auf der Grundlage von unzulässigen Rechtfertigungsgründen erfolgt sind. Besonders kritischen würden diese Datenverarbeitungen werden, je mehr Informationen gesammelt und miteinander verbunden werden würden. In der Zukunft sei daher die Durchsetzbarkeit von Schadenersatz- und Unterlassungsansprüchen, aufgrund der zuvor beschriebenen Rechtsprechung, durchaus möglich.¹⁹⁷

Als weitere wichtige Erkenntnis kann aus der Entscheidung abgeleitet werden, dass der EuGH die Ansicht vertritt, dass bei dem Vorliegen eines sensiblen Datums in einem Datensatz die Verarbeitung des gesamten Datensatzes gemäß Art 9 Abs 1 DSGVO untersagt ist, sofern keine der Ausnahmen des Art 9 Abs 2 DSGVO zutrifft.¹⁹⁸¹⁹⁹

Golland äußert sich kritisch zu dieser Auslegung, würde sie doch dazu führen, dass Unternehmen, welche Daten von ihren Kunden verarbeiten, möglicherweise mittelbar sensible Informationen verarbeiten würden und daher einen der Rechtfertigungsgründe für sensible Daten erfüllen müssten, damit die Datenverarbeitung nicht rechtswidrig wäre. Als Beispiel führt *Golland* einen Bestelldienst an, welcher an eine Klinik liefern würde (im Sinne der Kategorie der Gesundheitsdaten), sowie den Onlineversand von erotischen Produkten (sexuelle Orientierung). In diesen Fällen sei die Anwendbarkeit der besonderen Bestimmungen zur Verarbeitung von sensiblen Daten möglich. Darüber hinaus könnten sich für Kleinunternehmen Probleme hinsichtlich der Datenverarbeitungsverzeichnisse ergeben sowie der möglichen Anforderung der Durchführung einer

¹⁹⁵ Siehe *Hense*, KuR 2023, 556 (559).

¹⁹⁶ Siehe *Hense*, KuR 2023, 556 (559); *Golland*, Kompetenz nationaler Wettbewerbsbehörden zur Feststellung eines Verstoßes gegen die DS-GVO, MMR 2023, 669 (681).

¹⁹⁷ Siehe *Hense*, KuR 2023, 556 (559).

¹⁹⁸ Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 89; *Golland*, MMR 2023, 669 (682).

¹⁹⁹ Siehe auch „Mischdaten“ 4.1.2.1.

Datenschutzfolgenabschätzung.²⁰⁰ Seiner Ansicht folgend wäre daher eine Differenzierung – ein sogenanntes „Stufenkonzept“, welches über die Anwendung des Art 9 DSGVO entscheidet – bei mittelbar sensiblen Daten sinnvoll. Diese Differenzierung solle nur dann zu einer Anwendung des Art 9 DSGVO führen, wenn die Daten in einem sensiblen Kontext verarbeitet werden müssten oder eine „Sensibilitätsprognose“ würde ergeben, dass die Anwendung der Bestimmungen zu sensiblen Daten zum Schutz des Betroffenen geboten seien. Bei dieser „Sensibilitätsprognose“ seien die an der Verarbeitung beteiligten Personen, einschließlich der potenziellen Datenempfänger, einzubeziehen.²⁰¹

Wie bereits von *Gosch* formuliert wurde, vertritt auch *Hense* die Ansicht, dass das wohl effektivste Gegenmittel, um die Problematik der sensiblen Daten vermeiden zu können, wäre, dass sich die Verantwortlichen noch stärker auf die Grundsätze der Datenminimierung besinnen sowie Systeme verwenden sollten, welche die Anforderungen des „Privacy by Design“ sowie „Privacy by Default“ erfüllen.²⁰²

4.2.6 Judikatur: EuGH Entscheidung C-667/21, vom 21.12.2023

Dieser, Ende 2023 ergangenen, Entscheidung des EuGH liegt ein Ausgangsverfahren in Deutschland zu Grunde, welches sich im Wesentlichen mit der Frage auseinandersetzte, unter welchen Voraussetzungen die Verarbeitung von Gesundheitsdaten im Sinne der DSGVO zulässig ist. Bei der gegenständlichen Verarbeitung nahm der Verantwortliche, der Medizinische Dienst der Krankenversicherung Nordrhein, eine Art „Doppelfunktion“ ein, da der MDK Nordrhein sowohl Arbeitgeber des Klägers als auch Ersteller des medizinischen Gutachtens, betreffend der Arbeitsunfähigkeit des Klägers, war.²⁰³

Darüber hinaus sollte die Frage beantwortet werden, ob der Schadenersatzanspruch gemäß Art 82 Abs 1 DSGVO lediglich eine Ausgleichfunktion darstellen soll, oder auch „Strafcharakter“ hat und der Grad des Verschuldens des Verantwortlichen bei der Höhe des Schadenersatzes zu berücksichtigen ist.²⁰⁴

Die gegenständliche Entscheidung ist für die Erörterung der Forschungsfrage dieser Arbeit insbesondere von Bedeutung, da sich das Judikat mit dem Umfang des Verarbeitungsverbots des Art 9 Abs 1 DSGVO auseinandersetzt und sich hieraus Rückschlüsse auf andere Anwendungsfälle, wie bei der Verarbeitung von Bildaufnahmen, schließen lassen.

²⁰⁰ Siehe *Golland*, MMR 2023, 669 (681).

²⁰¹ Siehe *Golland*, MMR 2023, 669 (681).

²⁰² Siehe *Hense*, KuR 2023, 556 (559).

²⁰³ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 19ff.

²⁰⁴ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 32ff.

4.2.6.1 *EuGH Entscheidung C-667/21, vom 21.12.2023: Ausgangsverfahren u Vorlagefragen*

Der MDK Nordrhein hat unter anderem die gesetzliche Aufgabe, medizinische Gutachten zur Beseitigung von Zweifeln bei der Arbeitsunfähigkeit von versicherten Personen, die in den Zuständigkeitsbereich des MDK Nordrhein fallen, zu erstellen. Dies ist auch dann der Fall, wenn die Gutachten eigene Mitarbeiter:innen des MDK Nordrhein betreffen.²⁰⁵ Für solche Fälle besteht eine eigene Dienstanweisung, damit solche Daten von Mitarbeiter:innen zB nur von einer eingeschränkten Anzahl an Personen verarbeitet werden können.²⁰⁶

Der Kläger in Deutschland war bei MDK Nordrhein in der IT beschäftigt.²⁰⁷ Der Krankenversicherer des Klägers beauftragte den MDK Nordrhein mit der Erstellung eines Gutachtens des Klägers. Der Kläger erfuhr von dem Gutachten und bat einen Kollegen aus der IT-Abteilung ihm Fotos von dem Gutachten aus dem digitalen Archiv zu übermitteln.²⁰⁸ Der Kläger war von der rechtswidrigen Verarbeitung seiner Gesundheitsdaten überzeugt und forderte daher eine Entschädigung in der Höhe von EUR 20.000,- von MDK Nordrhein.²⁰⁹ Der Kläger erhob schließlich Klage am Arbeitsgericht Düsseldorf über die oben genannte Summe und stütze seine Forderungen ua auf Art 82 Abs 1 DSGVO.

Im Wesentlichen wurde vorgebracht, dass das Gutachten von einem anderen medizinischen Dienst hätte erstellt werden müssen, damit sichergestellt werden könnte, dass Kolleg:innen des Klägers keinen Zugang zu den Gesundheitsdaten erlangen könnten. Darüber hinaus seien die Sicherheitsmaßnahmen, betreffend die Datenverarbeitung dieser Gesundheitsdaten, unzureichend gewesen. Aufgrund dieses Verstoßes gegen den Schutz solcher Daten, stünde dem Kläger Ersatz für den ihm entstandenen materiellen und immateriellen Schaden zu.²¹⁰

Der MDK Nordrhein brachte im Wesentlichen vor, dass die Verarbeitung der Daten im Einklang mit den anwendbaren Bestimmungen erfolgt wäre.²¹¹

Sowohl in erster Instanz als auch in der Berufung wurde die Klage abgewiesen, weshalb Revision bei dem vorlegenden Gericht, dem Bundesarbeitsgericht in Deutschland, eingebracht wurde.²¹² Das vorlegende Gericht vertritt die Ansicht, dass in dem Erstellen des Gutachtens durch MDK Nordrhein eine Verarbeitung im Sinne der einschlägigen Bestimmungen der DSGVO besteht. Das vorlegende Gericht prüfte, ob die oben beschriebenen Datenverarbeitungen unter einer der in Art 9 Abs 2 DSGVO

²⁰⁵ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 19.

²⁰⁶ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 20.

²⁰⁷ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 21.

²⁰⁸ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 22.

²⁰⁹ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 23.

²¹⁰ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 24.

²¹¹ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 25.

²¹² Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 26.

genannten Ausnahmen subsumiert werden können. So sei beispielsweise Art 9 Abs 2 lit b DSGVO nicht einschlägig, da die Verarbeitung in der „Eigenschaft als Arbeitgeber“ nicht erforderlich gewesen sei. Auch die Ausnahme in Art 9 Abs 2 lit h DSGVO sei wohl nicht anzuwenden, da die Verarbeitung von einem „neutralen Dritten“ hätte durchgeführt werden müssen.

Im Falle, dass Art 9 Abs 2 lit h DSGVO doch anzuwenden sei, führt das vorlegende Gericht an, dass die Erfüllung der Anforderungen des Art 9 Abs 3 DSGVO nicht ausreichen würden und MDK Nordrhein hätte sicherstellen müssen, dass keiner der Kolleg:innen des Klägers Zugang zu den Gesundheitsdaten des Klägers hätte.²¹³

Darüber hinaus möchte das vorlegende Gericht wissen, ob zusätzlich zu einem Ausnahmetatbestand des Art 9 Abs 2 DSGVO auch eine der Voraussetzungen des Art 6 Abs 1 DSGVO erfüllt sein muss.²¹⁴

Bezüglich eines möglichen Schadenersatzes gemäß Art 82 Abs 1 DSGVO möchte das vorlegende Gericht unter anderem wissen, ob neben der Ausgleichsfunktion des Schadenersatzes auch die abschreckende Wirkung bzw der „Strafcharakter“ sowie der Grad des Verschuldens des Verantwortlichen zu berücksichtigen seien.²¹⁵

Da im Zuge dieser Arbeit insbesondere die Beantwortung der Vorlagefragen von Bedeutung ist, welche sich mit der Anwendbarkeit des Verarbeitungsverbots gemäß Art 9 Abs 1 DSGVO auseinandersetzt, wird auf genauere Ausführungen zu den anderen Vorlagefragen verzichtet.²¹⁶

4.2.6.2 EuGH Entscheidung C-667/21, vom 21.12.2023: Entscheidung

Der EuGH beantwortet die erste Vorlagefrage im Wesentlichen damit, dass Art 9 Abs 2 lit h DSGVO in Verbindung mit Abs 3 dieses Artikels die Anwendbarkeit von Art 9 Abs 2 lit h DSGVO keinesfalls in Situationen ausschließt, in denen eine Stelle für medizinische Begutachtung die Gesundheitsdaten eines Arbeitnehmers, betreffend seine Arbeitsfähigkeit, als Medizinischer Dienst verarbeitet und nicht in seiner Rolle als Arbeitgeber.

Dies begründet der EuGH unter anderem damit, dass zwar das grundsätzliche Verbot der Verarbeitung von „sensiblen Daten“ gemäß Art 9 Abs 1 DSGVO einen erhöhten Schutz vor Datenverarbeitungen gewährleisten soll, Art 9 Abs 2 lit a-j DSGVO jedoch eine abschließende Liste an Ausnahmen dieses Grundsatzes vorsehen würde.²¹⁷

²¹³ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 27ff.

²¹⁴ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 31.

²¹⁵ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 32ff.

²¹⁶ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 35.

²¹⁷ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 41f.

Der Ausnahmetatbestand des Art 9 Abs 2 lit h DSGVO würde zudem in Verbindung mit Art 9 Abs 3 DSGVO die Verarbeitung von sensiblen Daten mit einer Reihe an Voraussetzungen streng reglementieren.²¹⁸ Dementsprechend wäre die Datenverarbeitung unter anderem an die Zwecke, welche in Art 9 Abs 2 lit h DSGVO aufgezählt sind, gebunden. Darüber hinaus habe die Datenverarbeitung aufgrund von bestimmten Rechtsgrundlagen zu erfolgen und die zu einer solchen Verarbeitung von Daten berechtigten Personen der Geheimhaltungspflicht nach Art 9 Abs 3 DSGVO zu unterliegen.²¹⁹ Weder aus dem Wortlaut noch aus der Entstehungsgeschichte des Art 9 Abs 2 lit h DSGVO würde sich ergeben, dass die gegenständliche Ausnahmebestimmung einem „neutralen Dritten“ vorbehalten sei und daher nicht für den Arbeitgeber einer betroffenen Person anzuwenden wäre.²²⁰ Betreffend der „Doppelfunktion“ des Verantwortlichen weist der EuGH darauf hin, dass es von entscheidender Bedeutung ist, zu welchem Zweck die entsprechenden Daten verarbeitet werden würden.²²¹ Darüber hinaus ist der Zusammenhang der Ausnahmebestimmung in der DSGVO sowie die Ziele, welche die Datenschutzgrundverordnung verfolgt, zu berücksichtigen.²²² Die Ausnahmetatbestände des Art 9 Abs 2 DSGVO seien unabhängig voneinander auf ihre Anwendbarkeit zu prüfen und grundsätzlich eng auszulegen.²²³ Die Beachtung des allgemeinen Verarbeitungsverbots gemäß Art 9 Abs 1 DSGVO darf jedoch nicht dazu führen, dass der Anwendungsbereich anderer Bestimmungen der DSGVO, wie auch des Art 9 Abs 2 DSGVO, in einer solchen Weise eingeschränkt wird, dass dies deren „eindeutigem Wortlaut“ zuwiderlaufen würde.²²⁴ Die Anforderung, dass Art 9 Abs 2 lit h DSGVO auf Fälle beschränkt sei, in denen die Gesundheitsdaten durch einen „neutralen Dritten“ verarbeitet werden, würde jedoch eine solche zusätzliche Anforderung darstellen, welche keinesfalls aus dem eindeutigen Wortlaut der betroffenen Bestimmung hervorgeht.²²⁵ Des Weiteren stellt das Recht auf den Schutz der personenbezogenen Daten kein uneingeschränktes Recht dar, da es mit anderen Grundrechten abzuwägen ist.²²⁶ Aus den Erwägungsgründen 52 und 53 der DSGVO lässt sich zudem ableiten, dass die Verarbeitung von sensiblen Daten unter anderem zu bestimmten gesundheitlichen Zwecken zulässig ist.²²⁷ Der europäische Gesetzgeber hat mit Art 9 Abs 2 lit h DSGVO daher eine Ausnahmebestimmung vom allgemeinen Verarbeitungsverbots von sensiblen Daten, unter besonderen Voraussetzungen und

²¹⁸ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 44.

²¹⁹ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 44.

²²⁰ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 45.

²²¹ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 46.

²²² Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 49.

²²³ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 47ff.

²²⁴ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 51.

²²⁵ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 51.

²²⁶ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 54.

²²⁷ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 56.

Garantien, vorgesehen. Das die Verarbeitung von Gesundheitsdaten durch einen „neutralen Dritten“ zu erfolgen hat, geht aus den entsprechenden Bestimmungen nicht hervor.²²⁸

Die zweite Frage beschäftigte sich damit, ob sich aus den Bestimmungen der DSGVO ergibt, dass ein Verantwortlicher einer Verarbeitung von Gesundheitsdaten, welche sich auf Art 9 Abs 2 lit h DSGVO stützt, gewährleisten muss, dass keine, mit der betroffenen Person zusammenarbeitende, Person Zugang zu den verarbeiteten Gesundheitsdaten hat.²²⁹ Für die Verarbeitung entsprechender sensibler Daten hat der Unionsgesetzgeber in Art 9 Abs 2 lit h DSGVO sowie insbesondere Art 9 Abs 3 DSGVO spezifische Schutzmaßnahmen definiert. Dem Wortlaut von Art 9 Abs 3 DSGVO dürfen daher keine, nicht bereits genannten, Anforderungen hinzugefügt werden.²³⁰ Solche zusätzlichen Anforderungen könnten sich jedoch aus dem nationalen Recht, sofern diese aufgrund einer Öffnungsklausel erlassen wurden, ergeben. Aus Art 9 Abs 2 lit h DSGVO ergibt sich eine entsprechende Verpflichtung nicht.²³¹

Mit der dritten Vorlagefrage sollte im Wesentlichen geklärt werden, ob bei der Verarbeitung von Gesundheitsdaten, zusätzlich zu den Anforderungen des Art 9 Abs 2 lit h DSGVO, auch mindestens eine der Rechtmäßigkeitsvoraussetzungen des Art 6 Abs 1 DSGVO erfüllt sein muss.²³² Der EuGH stellt klar, dass eine auf Art 9 Abs 2 lit h DSGVO gestützte Verarbeitung jedenfalls auch die Grundsätze der Verarbeitung gemäß Art 5 Abs 1 DSGVO, die in Art 6 Abs 1 DSGVO genannten Pflichten sowie mindestens eine der genannten Rechtmäßigkeitsvoraussetzungen erfüllen muss.²³³

Abschließend ist darauf hinzuweisen, dass der EuGH festgestellt hat, dass der Schadenersatzanspruch gemäß Art 82 Abs 1 DSGVO Ausgleichs- und keine Straffunktion hat.²³⁴ Der Grad des Verschuldens des Verantwortlichen ist für die Höhe des Schadenersatzes nicht zu berücksichtigen.²³⁵

4.2.6.3 Eigene Überlegungen zur EuGH Entscheidung C-667/21, vom 21.12.2023

Aus der gegenständlichen Entscheidung des EuGH ergibt sich meines Erachtens ein guter Ausblick auf die zukünftige Judikaturlinie des Höchstgerichts. In den EuGH Entscheidungen C-252/21 vom 04.06.2023 sowie C-184/20 vom 01.08.2022 legte der EuGH das Verbot der Verarbeitung von

²²⁸ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 57.

²²⁹ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 60.

²³⁰ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 62.

²³¹ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 70.

²³² Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 71.

²³³ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 78f.

²³⁴ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 87.

²³⁵ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 103.

sensiblen Daten gemäß Art 9 Abs 1 DSGVO weit aus, um ua einen erhöhten Schutz gegenüber Datenverarbeitungen zu gewährleisten.²³⁶

Gegenläufig dazu verweist der EuGH in seiner Entscheidung C-667/21 vom 21.12.2023 ausdrücklich darauf, dass die Beachtung des grundsätzlichen Verarbeitungsverbots nicht dazu führen darf, dass andere Bestimmungen der DSGVO, wie beispielsweise die Ausnahmerebestimmungen gemäß Art 9 Abs 2 DSGVO, dem Wortlaut zuwiderlaufend eingeschränkt werden.²³⁷ Des Weiteren bezieht sich der EuGH in seiner Argumentation ua darauf, dass das „Recht auf Schutz der personenbezogenen Daten“ kein uneingeschränktes Recht darstellt.²³⁸ Trotz des besonderen Schutzes von sensiblen Daten, soll deren Verarbeitung zulässig sein, sofern die Anforderungen einer der Ausnahmetatbestände erfüllt ist. Auch wenn in der gegenständlichen Entscheidung die Einstufung von bestimmten personenbezogenen Daten als sensible Daten unstrittig war, da davon ausgegangen wurde, dass es sich bei den verarbeiteten Daten um Gesundheitsdaten im Sinne des Art 4 Z 15 DSGVO handelt, können die gewonnen Erkenntnisse auf die Problematik bezüglich der Einstufung von Bildaufnahmen als sensible Daten übertragen werden. Meines Erachtens gibt dieses Urteil Aussicht darauf, dass der EuGH keine „unverhältnismäßige“ Ausdehnung des Datenschutzes, wie es manche Stimmen in der Literatur befürchten,²³⁹ anstrebt. In seiner Entscheidung berücksichtigt der EuGH auch die Ziele, welche der DSGVO zugrunde liegen.²⁴⁰ Aus diesen Gründen deutet die Entscheidung mE auf eine „verarbeitungsfreundlichere“ Auslegung der gegenständlichen Normen hin. In diesem Zusammenhang ist auch zu berücksichtigen, dass eine besonders „weite“ Auslegung der Definition von sensiblen Daten, beispielsweise auch auf Bildaufnahmen, wohl zu einer praktischen „Verunmöglichung“ von vielen Anwendungsbereichen, in denen Bilder oder Videos verarbeitet werden, führen würde. Eine Einschränkung in dieser Art und Weise kann meines Erachtens kein Ziel der DSGVO sein, andernfalls hätte auch die Möglichkeit bestanden, eine solche Einschränkung von Bildverarbeitungen eindeutig zu formulieren.

5 Zusammenfassung und Ausblick

5.1 Zusammenfassung

Aus den zuvor beschriebenen Entscheidungen des EuGH (C-252/21 vom 04.06.2023, C-184/20 vom 01.08.2022 sowie C-667/21, vom 21.12.2023) können einige wesentliche Erkenntnisse für die Einstufung von Bildaufnahmen von natürlichen Personen als sensible Daten gewonnen werden. Geht

²³⁶ Vgl. EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 126; Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 70.

²³⁷ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 51.

²³⁸ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 54.

²³⁹ Siehe Kienle, LTZ 2023, 50 (67).

²⁴⁰ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 49.

man von den beiden unter Punkt 4.1.1 sowie 4.1.2 genannten Interpretationsstandpunkten, welche sich grob in einen „objektiven“ und einen „subjektiven“ Ansatz zusammenfassen lassen, aus, dann könnte man die Ansicht vertreten, dass der EuGH einer objektiven Auslegung folgt.

In der weiter zurückliegenden Entscheidung des EuGH vom 01.08.2022, berücksichtigte dieser bei seiner Prüfung weder den Verwendungszusammenhang (bzw objektiver Verarbeitungskontext) noch den subjektiven Zweck der Verarbeitung durch den Verarbeiter. Wie *Kienle* es formuliert, werden diese beiden Ansätze durch den EuGH unausgesprochen zurückgewiesen, beide würden daher Art 9 Abs 1 DSGVO nicht einschränken.²⁴¹ In seiner jüngeren Entscheidung vom 04.06.2023 wird der EuGH noch deutlicher und spricht die Zurückweisung offen aus. Die entsprechenden Datenverarbeitungen seien unabhängig von ihrem „erklärten Zweck“ gemäß Art 9 Abs 1 DSGVO zu verbieten.²⁴²

Ob an dieser Stelle noch Spielraum für den „objektiven Verwendungszusammenhang“ besteht, wie ihn beispielsweise *Jahnel* formuliert hat,²⁴³ ist fraglich. Nachdem *Gosch* jedoch bereits nach der Entscheidung in der Sache C-184/20 (Vyriausioji tarnybinės etikos komisija) die Ansicht vertrat, dass der EuGH bei der Berücksichtigung des objektiven Verwendungszusammenhangs zu einem anderen Ergebnis hätte kommen müssen, ist davon auszugehen, dass das europäische Höchstgericht ein solches Kriterium bei seiner Prüfung nicht herangezogen hat.²⁴⁴

Zusammenfassend kann daher gesagt werden, dass weder durch objektive noch subjektive Merkmale, welche sich auf den Verarbeitungskontext oder Zweck beziehen, der Anwendungsbereich des Art 9 Abs 1 DSGVO im Sinne dieser EuGH Entscheidungen eingeschränkt wird. Daraus kann des Weiteren geschlossen werden, dass die in dem Leitfaden der EDSA aus dem Jahr 2019 betreffend „Verarbeitung von personenbezogenen Daten durch Videogeräte“ vertretene Argumentation, dass es bei der Anwendung von Art 9ff DSGVO auf den Verarbeitungszweck bei Videomaterial ankäme, vor dem Hintergrund der gegenständlichen Rechtsprechung als überholt angesehen werden muss.²⁴⁵

Meines Erachtens ist auch hervorzuheben, dass der EuGH mit der zuvor besprochenen Entscheidung vom 04.06.2023 klarstellt, dass das Verbot der Verarbeitung von sensiblen Daten auch in den Fällen anwendbar ist, in denen die offengelegte Information unrichtig ist.²⁴⁶ (*Bergauer* vertritt im Zusammenhang mit dem Abgrenzungskriterium der „hinlänglichen Sicherheit“ die Ansicht, dass es

²⁴¹ Siehe *Kienle*, LTZ 2023, 50 (67).

²⁴² Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 70.

²⁴³ Vgl *Jahnel* in DSGVO Art 9 DSGVO Rz 14.

²⁴⁴ Siehe *Gosch*, jusIT 2022/76, 183 (186f).

²⁴⁵ Vgl EDSA, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Rz 64.

²⁴⁶ Vgl EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 69.

hierbei nicht darauf ankäme, ob die getroffene Einschätzung schlussendlich zutreffend ist oder nicht.)²⁴⁷ Daraus ergibt sich, dass die offengelegten Informationen nicht auf ihre Richtigkeit überprüft werden müssen. Entscheidend sollte daher, im Sinne der Schlussanträge des Generalanwalts Rantos vom 20.09.2022, sein, dass eine solche Kategorisierung zu einem erheblichen Risiko für die Grundrechte und Grundfreiheiten der betroffenen Person führen kann. Dies könne unabhängig von dem jeweiligen Wahrheitsgehalt eintreten.²⁴⁸ Bisher war diese Ansicht beispielsweise durch den EDSA in seiner „Leitlinie 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien“ vertreten worden. In diesem Zusammenhang ging es um das gezielte Targeting von Nutzern und deren Einordnung in bestimmte politische Spektren. Die Richtigkeit einer solchen Einstufung sei im Sinne der EDSA-Leitlinie nicht relevant für die Anwendbarkeit des Art 9 DSGVO.²⁴⁹

Darüber hinaus ist die jüngste der zuvor beschriebenen Entscheidungen des EuGH etwas zurückhaltender betreffend die Auslegung des Verarbeitungsverbots gemäß Art 9 Abs 1 DSGVO. Mit diesem Urteil scheint das Höchstgericht eine „verarbeitungsfreundlichere“ Auslegung der Bestimmungen zu sensiblen Daten anzustreben.²⁵⁰

5.2 Mögliche Auswirkungen auf die Praxis

Die beiden zuvor genauer besprochenen Entscheidungen des EuGH können meines Erachtens entscheidenden Einfluss auf die datenschutzrechtliche Handhabung von Bilder- und Videoaufnahmen haben.

Beispielsweise vertritt *Assion* die Ansicht, dass die EuGH Entscheidung C-252/21 vom 04.06.2023 große Auswirkungen auf die Problematik der Einordnung von Videoüberwachung und Bildaufnahmen von natürlichen Personen haben könnte.²⁵¹ In der Vergangenheit wurde von vielen Seiten, insbesondere für Bildaufnahmen, die Anwendbarkeit des besonderen Schutzes des Art 9 Abs 1 DSGVO verneint. Wie bereits unter Punkt 4.1.1 beschrieben, vertrat im Jahr 2019 auch der Europäische Datenschutzausschuss eine Auslegung, welche sich an dem Zweck der Verarbeitung orientierte. Diese Auslegung wurde nunmehr durch den EuGH indirekt abgelehnt. Die möglichen Folgen für Videoüberwachung (welche in diesem Zusammenhang wohl auch für „reguläre“ Bildaufnahmen übernommen werden können), gibt der EDSA unter Rz 70 des Leitfadens selbst an. Die in Art 9 Abs 2 DSGVO angeführten Ausnahmetatbestände dürften in der Regel ungeeignet für die

²⁴⁷ Siehe *Bergauer*, *jusIT* 2016/103, 241 (246).

²⁴⁸ Siehe GA RANTOS 20.09.2022, C-252/21 Rz 40.

²⁴⁹ Siehe EDSA, Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien“, Version 2.0, Rz 125 <edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_de_0.pdf> (22.01.2024).

²⁵⁰ Siehe EuGH 21.12.2023, C-667/21 (MDK Nordrhein) Rz 51ff.

²⁵¹ Siehe *Assion*, Die Entwicklung des Datenschutzrechts, *NJW* 2023, 2619 (2621).

Rechtfertigung von Videoüberwachungen sein. Insbesondere würde die bloße Tatsache, dass eine Person den Erfassungsbereich einer Kamera betritt, nicht darauf hindeuten, dass die Person im Sinne des Art 9 Abs 2 lit e DSGVO sensible Daten von sich (freiwillig) öffentlich macht.²⁵² Für die tatsächliche Verarbeitung von sensiblen Daten dürften jedoch auch die (möglicherweise) einschlägigen Ausnahmetatbestände des Art 9 Abs 2 DSGVO ungeeignet sein, da auch diese keine dauerhaft angelegte und über den Einzelfall hinausgehende Videoüberwachung zu rechtfertigen vermögen.²⁵³

Kienle sieht aus einer solch weiten Auslegung der sensiblen Daten, wie sie aus den jüngsten EuGH-Entscheidungen hervorgeht, erhebliche Folgen für die Privatwirtschaft, insbesondere in den Bereichen der Legal-Tech. In Ermangelung eines Ausnahmetatbestandes, welcher die Vertragserfüllung bzw die Interessenabwägung vorsieht, bliebe unter diesen Umständen privaten Verantwortlichen nur die Einwilligung des Betroffenen. Dieser Ausnahmetatbestand sei in der Regel für die entsprechenden Verarbeitungen jedoch nicht einschlägig. Das Verbot der Datenverarbeitung gemäß Art 9 Abs 1 DSGVO sei daher oft nicht bloß „relativ“ (entgegen der Schlussanträge des GA Pikamäe in der Rechtssache C-184/20 vom 09.12.2021). Darüber hinaus könnte gemäß der Ansicht von *Kienle* diese weite Auslegung von sensiblen Daten auch den „Data Governance Act“ sowie „Data Act“ beeinflussen.²⁵⁴ Weiters äußerten sich, insbesondere bezüglich des Bereichs der KI-Anwendungen, einige Autoren kritisch gegenüber der weiten Auslegung der besonderen Kategorien personenbezogener Daten. Es besteht die Befürchtung, dass durch KI-Anwendungen massenhaft sensible Daten verarbeitet werden könnten.²⁵⁵ Insbesondere der schnell steigende technische Fortschritt habe auch zur Folge, dass beispielsweise durch Anwendungen auf Smartphones eine Vielzahl an verschiedenen Daten der Nutzer verarbeitet werden würden. Dies würde dazu führen, dass das Verarbeitungsverbot gemäß Art 9 Abs 1 DSGVO, insbesondere in Anbetracht einer weiten Auslegung von sensiblen Daten, sehr viel häufiger zur Anwendung kommen könnte, da durch die erhöhte Anzahl an verarbeiteten Daten auch die Wahrscheinlichkeit zunehmen könnte, dass ein sensibles Datum unter diesen verarbeiteten Daten sein könnte. Insbesondere bei Fällen der „zufälligen Mitverarbeitung“ von sensiblen Daten, seien die Ausnahmetatbestände gemäß Art 9 Abs 2 DSGVO in der Regel nicht einschlägig.²⁵⁶

²⁵² Siehe *EDSA*, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Rz 70.

²⁵³ Vgl *Kienle*, LTZ 2023, 50 (67).

²⁵⁴ Siehe *Kienle*, LTZ 2023, 50 (67).

²⁵⁵ Vgl *Hessel/Dillschneider*, Datenschutzrechtliche Herausforderungen beim Einsatz von Künstlicher Intelligenz, RD 2023, 458 (461).

²⁵⁶ Vgl *Britz/Indenhuck/Langerhans*, Die Verarbeitung „zufällig“ sensibler Daten, ZD 2021, 559 (561).

Deiters vertritt die Ansicht, dass noch abzuwarten sei, wie die Gerichte und Datenschutzbehörden auf die weite Auslegung in der Rechtssache C-184/20 reagieren werden.²⁵⁷

Weitere praktische Auswirkungen könnten für Unternehmen unter anderem darin bestehen, dass beispielsweise Fotos von Mitarbeiter:innen, welche zB auf der unternehmenseigenen Website veröffentlicht werden, bisher in der Regel aufgrund berechtigten Interesses verarbeitet wurden.²⁵⁸ Bei einer Einstufung von Bilddateien als sensible Daten, müsste ein entsprechender Ausnahmetatbestand für die Verarbeitung einschlägig sein.

Ebenso verhält es sich bei der video- bzw fotografischen Dokumentation von Veranstaltungen und Ähnlichem. So verweist beispielsweise auch die WKO in ihren entsprechenden Mustererklärungen auf das Vorliegen eines berechtigten Interesses im Sinne des Art 6 Abs 1 lit f DSGVO betreffend Fotografie und Werbung.²⁵⁹ In der Zukunft könnte daher auch für solche Anwendungsfälle die Einwilligung der Personen das probateste Mittel für die Verarbeitung sein. Die Einwilligung würde in diesen Fällen jedoch aus Sicht des Verarbeiters den Nachteil mit sich bringen, dass diese durch die betroffenen Personen widerrufen werden könnte.

5.3 Eigene Interpretation und Ansätze

Wie unter Punkt 4.2 dieser Arbeit dargestellt wurde, stellt die jüngste Judikatur des EuGH betreffend sensible Daten die Vertreter:innen der Literatur und in weiterer Folge die Anwender:innen in der Praxis vor große Herausforderungen. Wie es bereits *Laimighofer* formuliert hat, werden daher weite Teile der aktuellen Literatur zu überdenken sein.²⁶⁰ Entsprechend den Entscheidungen des EuGH wird der Begriff der sensiblen Daten bzw das Verarbeitungsverbot des Art 9 Abs 1 DSGVO weiter auszulegen sein als von vielen Vertretern der Praxis gewünscht. Ob sich aus dieser Tatsache jedoch ergibt, dass der Datenschutz in dieser Hinsicht zu einem „absoluten Recht mutieren“ würde²⁶¹ und in Zukunft jedes Lichtbild einer Person ein sensibles Datum darstellen könnte,²⁶² bleibt abzuwarten.

In der Zukunft wird meines Erachtens jedoch nicht mehr auf den subjektiven Verwendungs- bzw Verarbeitungszweck des Verarbeiters abzustellen sein. Fortan sollte daher auf objektive Kriterien für die Kategorisierung von sensiblen Daten zurückgegriffen werden.

²⁵⁷ Siehe *Deiters*, DSB 2022, 247 (249).

²⁵⁸ Vgl *Goricnik*, Unter welchen Voraussetzungen ist es datenschutzrechtlich zulässig, Fotos von Mitarbeitern digital zugänglich zu machen?, *Dako* 2023/14, 21.

²⁵⁹ Siehe <wko.at/branchen/information-consulting/werbung-marktkommunikation/fotografie-und-werbung.html>.

²⁶⁰ Siehe *Laimighofer*, *jusIT* 2023, 102 (107).

²⁶¹ Siehe *Kienle*, *LTZ* 2023, 50 (67).

²⁶² Siehe *Gosch*, *jusIT* 2022/76, 183 (189).

Hierfür erscheint mir jedoch ein Kriterium wie das der „hinlänglichen Sicherheit“²⁶³ allein nicht ausreichend. Für Lichtbildaufnahmen ergibt sich mit diesem Abgrenzungsversuch das Problem, dass in vielen alltäglichen Fällen mit „hinlänglicher Sicherheit“ sensible Daten (beispielsweise Gesundheitsdaten) abgeleitet werden können und diese Daten, insbesondere bei Videoüberwachungen, in der Regel „zufällig“ verarbeitet werden.²⁶⁴ In diesem Zusammenhang kann als Beispiel die Bildaufnahme einer Person, welche eine Brille trägt, verwendet werden (wie bereits in diversen Artikeln, die sich mit diesem Thema auseinander gesetzt haben).²⁶⁵ Auch eine (zufällige) Lichtbildaufnahme eines Brillenträgers oder einer Person, die auf einen Rollstuhl angewiesen ist, lässt in der Regel mit hinlänglicher Sicherheit den Rückschluss auf eine Seh- bzw Gehschwäche des Abgelichteten zu. Daher könnte argumentiert werden, dass in einem solchen Fall eine Verarbeitung von sensiblen Daten erfolgt.²⁶⁶

Der Ansicht *Laimighofers* folgend, könnte in einem derartigen Foto (Person trägt Brille), wie es beispielsweise von einer Überwachungskamera aufgenommen wurde, keine Verarbeitung von sensiblen Daten gesehen werden. Dies würde erst zu dem Zeitpunkt zutreffen, an dem sich diese sensible Information einer konkreten Person zuordnen lässt.²⁶⁷ Bei einer Überwachungsbildaufnahme einer zufällig an der Kamera vorbeigehenden Person wäre eine solche Zuordnung nicht aufgrund der vorliegenden Daten möglich. Anders würde es sich gemäß dieser Ansicht wohl verhalten, wenn die abgelichtete Person der langjährige Mitarbeiter des videoüberwachten Unternehmens wäre. In dieser Konstellation könnte der Datensatz die Identifizierung der Person ermöglichen, welcher die sensible Information zugehörig ist.²⁶⁸

Auch wenn diese Überlegungen gut durchdacht scheinen, vermögen sie aus meiner Sicht dennoch nicht völlig zu überzeugen. Zwar wird in dieser Art der Auslegung vermieden, dass auf den subjektiven Verarbeitungszweck des Verarbeiters abgestellt wird, jedoch wird trotzdem ein gewisses subjektives Element des Verarbeiters für die Kategorisierung berücksichtigt. Die Informationen, welche aus einem Datensatz entnommen werden können und eine Identifikation der betroffenen Person ermöglichen, werden maßgeblich durch den Verarbeiter bestimmt bzw durch den jeweiligen Verarbeiter beeinflusst. In anderen Worten: abhängig vom jeweiligen Verarbeiter können ganz unterschiedliche Datensätze einer Person zugeordnet werden. Wäre in dem vorhin skizzierten

²⁶³ Vgl *Jahnel* in DSGVO Art 9 DSGVO Rz 21; *Bergauer*, *jusIT* 2016/103, 241 (246); *Schiff* in DS-GVO² Art 9 DSGVO Rz 14.

²⁶⁴ Vgl *Britz/Indenhuck/Langerhans*, *ZD* 2021 (10), 559 (562).

²⁶⁵ Vgl beispielsweise *Knyrim*, *jusIT* 2016/102, 235; *Bergauer*, *jusIT* 2016/103, 241; *Schneider/Schindler*, *ZD* 2018, 463.

²⁶⁶ Vgl *Ernst* in Paal/Pauly (Hrsg), DS-GVO BDSG³ Art 4 DSGVO Rz 109 (2021).

²⁶⁷ Siehe *Laimighofer*, *jusIT* 2023, 102 (106).

²⁶⁸ Siehe *Laimighofer*, *jusIT* 2023, 102 (105).

Beispiel der Brillenträger weithin für seinen exzentrischen Kleidungsstil bekannt, kann es nicht darauf ankommen, ob der jeweilige Verarbeiter diese Person erkennt und ihr das Gesundheitsdatum zuordnen kann. Entscheidend ist vielmehr, dass die sensible Information zugeordnet werden kann, sie also hervorgeht. Andernfalls müsste jeweils die gesamte Informationslage eines Verarbeiters berücksichtigt werden, um zu der Erkenntnis zu gelangen, ob die Verarbeitung von sensiblen Daten oder „normalen“ Daten erfolgt.

Darüber hinaus ergibt sich das Problem, dass die Pseudonymisierung von Daten nicht damit gleichzusetzen ist, dass ein Bild auf den ersten Blick nicht einer konkreten Person zugeordnet werden kann.²⁶⁹ Eine Pseudonymisierung im Sinne der DSGVO setzt unter anderem voraus, dass „[...] *die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können* [...]“²⁷⁰ Doch bei einer Bildaufnahme einer Person gehen eben diese Informationen, die eine Identifikation ermöglichen, unmittelbar aus dem Bild hervor. Auch wenn es sich nicht bei jedem Foto um biometrische Daten im Sinne der DSGVO handelt,²⁷¹ da nicht jede Bildaufnahme einer Person ein biometrisches Datum gemäß Definition darstellt,²⁷² kann durch ein einfaches Foto, aus dem auch ein Gesundheitsdatum hervorgeht, eine konkrete Person bestimmt werden. Es sind daher keine zusätzlichen Informationen notwendig, sondern diese Informationen (das Aussehen einer Person bestehend aus Gesichtsform, Auffälligkeiten etc) ergeben sich unmittelbar aus dem Bild. Daher erscheint es schwierig nachzuvollziehen, weshalb gemäß *Laimighofer* die Zuordnung eines sensiblen Datums zu einer konkreten Person beispielsweise aufgrund eines Namens ermöglicht werden würde und daher unter das Verarbeitungsverbot gemäß Art 9 Abs 1 DSGVO fallen würde,²⁷³ dies jedoch nicht bei einem einfachen Foto der Person der Fall sein sollte. Der Name einer Person beschreibt diese, kann jedoch von mehreren Personen zur gleichen Zeit getragen werden. Das Abbild eines Menschen kann meines Erachtens deutlich spezifischer auf eine Person schließen lassen, als der bloße Name (auch wenn es sich nicht um einen „Allerweltsnamen“ handelt). Man denke in diesem Zusammenhang an Bilder, welche von Vermissten oder Gesuchten ausgehängt werden.

Unabhängig von diesen Überlegungen, müsste sowohl der Name einer Person als auch eine Bildaufnahme mit bereits vorhandenem Wissen abgeglichen werden, um die konkrete Zuordnung einer Person zu ermöglichen. Sollte sowohl ein Gesundheitsdatum als auch der Name einer Person bekannt sein, müsste dieser trotz allem zB mit einer Suchmaschine abgeglichen werden (sofern die

²⁶⁹ Vgl *Laimighofer*, jusIT 2023, 102 (107).

²⁷⁰ Siehe Art 4 Z 5 DSGVO.

²⁷¹ Siehe Art 4 Z 14 DSGVO.

²⁷² Siehe ErwGr 51 VO (EU) 2016/679.

²⁷³ Vgl *Laimighofer*, jusIT 2023, 102 (106).

Person nicht bekannt ist), um das Gesundheitsdatum einer korrekten Person zuordnen zu können. Ganz ähnlich würde es sich bei einem Foto, welches auch ein Gesundheitsdatum einer Person enthält, verhalten. Mittels diverser Suchmaschinen können Bilddaten Personen zugeordnet werden. In der Folge wäre auch das Gesundheitsdatum einer konkreten Person zuzuordnen. Daher müssten auch den Regeln des Ansatzes von *Laimighofer* folgend, Bildaufnahmen und darin enthaltene sensible Daten einer konkreten Person zuzuordnen sein und daher unter das Verarbeitungsverbot von sensiblen Daten fallen. Aus diesem Grund bietet dieser Ansatz nur einen bedingten Mehrwert für die Einordnung von Bilddateien als sensible Daten.

Aus diesen Gründen stellt sich die Frage, ob in Anbetracht der zitierten EuGH-Judikatur nunmehr die von *Gosch* formulierte Formel „Sensibles Datum = Personenbezogenes Datum + geeignet, sensible Informationen indirekt zu offenbaren“ für die Einordnung von Bilddateien anzuwenden ist.

Im Umkehrschluss könnte dies dazu führen, dass quasi jedes Lichtbild in diese besondere Kategorie fallen könnte.²⁷⁴ Meines Erachtens ist dies nicht ohne weiteres der Fall.

Würde man die Definitionen der besonderen Kategorien personenbezogener Daten sehr weit verstehen, könnte man zu der Erkenntnis gelangen, dass beispielsweise auch ein Bild einer Person, die keine klar erkennbaren krankheitsbedingten Anzeichen zeigt, ein Gesundheitsdatum darstellen könnte (etwas, wenn auf einem Bild eine Person ohne Gehhilfe, etc erkennbar ist). *Bergauer* vertritt beispielsweise die Ansicht, dass auch die Information darüber, dass eine Person völlig gesund sei, ein Gesundheitsdatum in Sinne der DSGVO darstellen kann. Hierauf würde schon der positive Begriff „Gesundheit“ gegenüber „Krankheit“ hindeuten.²⁷⁵ Dies würde in der weiteren Folge dazu führen, dass eine Flut an verschiedenen Informationen als sensible Daten einzustufen wäre. Demgegenüber folgt beispielsweise *Schulz* dem Ansatz, dass aufgrund des Fehlens eines erhöhten Gefährdungspotentials des Aussagegehalts die Einordnung als besonders schützenswerte Information nicht gegeben sei. Daher sollte der „beschwerdefreie Zustand“ nicht erfasst sein.²⁷⁶ Diese grundsätzlichen Überlegungen können meines Erachtens auch für die Kategorisierung von Lichtbildaufnahmen relevant sein.

Der EuGH verweist in seiner Entscheidung C-184/20 vom 01.08.2022 darauf, dass die unionsrechtlichen Vorschriften nicht nur nach deren Wortlaut, sondern auch ihr Kontext und ihre jeweiligen Ziele für die Auslegung zu berücksichtigen sind.²⁷⁷ Des Weiteren wird mit Erwägungsgrund

²⁷⁴ Siehe *Gosch*, *jusIT* 2022/76, 183 (189).

²⁷⁵ Siehe *Bergauer*, *jusIT* 2016/103, 241 (246); Vgl *Jahnel*, Kommentar zur Datenschutz-Grundverordnung (DSGVO) Art 4 DSGVO Rz 4 (2021); kritisch hierzu *Schulz* in DS-GVO / BDSG³ Art 9 DSGVO Rz 20.

²⁷⁶ Siehe *Schulz* in DS-GVO / BDSG³ Art 9 DSGVO Rz 20.

²⁷⁷ Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 121.

51 der DSGVO darauf verwiesen, dass Verarbeitungen aufgrund der „[...] besonderen Sensibilität der betreffenden Daten einen besonders schweren Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen können.“²⁷⁸ Ähnlich verweist der EuGH in der Entscheidung C-252/21 (Meta Platforms) vom 04.06.2023 auf die erheblichen Risiken bei der Verarbeitung von sensiblen Daten für die Grundrechte und Grundfreiheiten der betroffenen Personen.²⁷⁹ Entscheidend für die kontextualisierte Auslegung des Verarbeitungsverbots gemäß Art 9 Abs 1 DSGVO ist meines Erachtens die besondere Sensibilität der Daten sowie die (potentiellen) schwerwiegenden Eingriffe in die Grundrechte.

Berücksichtigt man dieses Kriterium nun bei dem zuvor beschriebenen Beispiel (Lichtbildaufnahme einer gesunden Person), so muss man zu der Erkenntnis kommen, dass selbst wenn man aus diesem Foto ein Gesundheitsdatum über die Person ableiten kann, es sich bei der Verarbeitung dieser Daten sicherlich um keinen (potenziell) schwerwiegenden Eingriff in die Grundrechte der abgelichteten Person handeln kann. Das erhöhte Schadens- und Diskriminierungspotential,²⁸⁰ welches meines Erachtens für den erhöhten Verarbeitungsschutz entscheidend ist, würde sich in einem solchen Fall nur äußerst unwahrscheinlich realisieren.

Diese Überlegungen können auch auf das häufig zitierte Beispiel des Fotos eines Brillenträgers übertragen werden. Auch wenn es Konstellationen gibt, in denen Personen auch ohne eine Sehschwäche eine Brille tragen, kann mittels gedanklicher Kombination auf dieses Gesundheitsdatum (Sehschwäche) geschlossen werden. Auf die Richtigkeit dieser Kombination kommt es ohnedies nicht an.²⁸¹ Aus dem Bild geht daher ein Gesundheitsdatum einer Person hervor. Die Anwendung des Verarbeitungsverbots für sensible Daten entspricht meines Erachtens dennoch nicht der Interpretation der entsprechenden Normen der DSGVO, da auch in einem solchen Fall die Schutzbedürftigkeit der betroffenen Person nicht gegeben ist. Natürlich können Situationen bestehen, in denen Personen aufgrund ihrer Sehschwäche Diskriminierung erfahren, jedoch verwirklicht sich meines Erachtens nicht das erhöhte Diskriminierungsrisiko,²⁸² welches für sensible Daten bestehen kann. Für die Eignung zur Verwirklichung dieses Risikos soll nicht nur der jeweilige objektive Kontext, in dem die Datenverarbeitung erfolgt berücksichtigt werden, sondern ein möglichst breites Spektrum für die Risikobehaftung der Verarbeitung für den Betroffenen berücksichtigt werden.

²⁷⁸ Siehe EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija) Rz 121.

²⁷⁹ Siehe EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 70.

²⁸⁰ Vgl Frenzel in DS-GVO BDSG³ Art 9 DSGVO Rz 6.

²⁸¹ Vgl EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 69.

²⁸² Vgl Kastelitz/Hötzendorfer/Tschohl in DatKomm Art 9 DSGVO Rz 13.

Durch diese Überlegungen könnte insbesondere erklärt werden, weshalb das Gesundheitsdatum, dass eine Person keine äußeren Anzeichen einer Krankheit zeigt und daher „gesund“ ist, nicht unter den besonderen Schutz der sensiblen Daten fällt. Ebenfalls könnte bestätigt werden, dass die Information eine nicht „stigmatisierte“ sexuelle Orientierung zu haben, nicht dem Verarbeitungsverbot gemäß Art 9 Abs 1 DSGVO unterliegt. Es ist jedoch darauf zu achten, dass durch diese Überlegungen zu dem objektiven Risiko eines Betroffenen keine Interessenabwägung zwischen dem Verarbeiter und dem Betroffenen zu erfolgen hat. Die Beurteilung des Risikopotentials hat im Zweifel zugunsten des Betroffenen zu erfolgen. Im Zusammenspiel mit dem Kriterium der „hinlänglichen Sicherheit“ (bzw ähnliche Ansätze, die zu diesem Spektrum gezählt werden können),²⁸³ könnte die hier beschriebene Überlegung dennoch zu einer gewissen Reduktion des weiten Anwendungsbereichs der sensiblen Daten führen.

Nichtsdestotrotz vermag es diese teleologische Reduktion nicht, eine Vielzahl an (möglicherweise) kritischen Verarbeitungen im Zusammenhang mit Lichtbildaufnahmen zu rechtfertigen. Das Foto einer Person, welche beispielsweise auf einen Rollstuhl angewiesen ist, birgt zweifelsfrei ein gewisses Diskriminierungspotential für die betroffene Person und stellt darüber hinaus ein Gesundheitsdatum dar. Folglich müsste auch nach diesen Überlegungen in einem solchen Fall der Anwendungsbereich des Art 9 Abs 1 DSGVO gegeben sein. Insbesondere durch Videoüberwachungen können sich eine Vielzahl an verschiedenen Verarbeitungsszenarien ergeben, in welchen der besondere Schutzbedarf nicht ausgeschlossen werden könnte.

6 Conclusio

Die in dieser Arbeit genauer aufgezeigte Judikatur, insbesondere die jüngsten einschlägigen Entscheidungen des EuGH, verdeutlicht die große Herausforderung, welche mit der Kategorisierung von sensiblen Daten einhergeht. Ganz besonders gilt diese Problematik weiterhin für die Verarbeitung von Bilddateien. Die Informationsdichte ist bei modernen Lichtbildaufnahmen ausgesprochen hoch und der technische Fortschritt wird die Verarbeitungsmöglichkeiten von Bildaufnahmen weiter erhöhen. Auf der anderen Seite scheinen die bisher in der Praxis stark vertretenen verarbeitungsfreundlichen Ansätze, welche an den Verarbeitungszweck bzw den Verwendungszusammenhang der Datenverarbeitung angesetzt haben, nicht länger ohne weiteres haltbar.²⁸⁴ Der EuGH stellt klar, dass für die Beurteilung, ob sensible Daten verarbeitet werden, objektive Kriterien herangezogen werden sollen.²⁸⁵ Durch dieses Bekenntnis zu einer weiten Auslegung des Anwendungsbereichs der sensiblen Daten bleibt äußerst wenig Spielraum für

²⁸³ Vgl *Bergauer*, *jusIT* 2016/103, 241 (246); *Deiters*, *DSB* 2022, 247 (249).

²⁸⁴ Vgl *Laimighofer*, *jusIT* 2023, 102 (107).

²⁸⁵ Vgl EuGH 04.06.2023, C-252/21 (Meta Platforms) Rz 70.

Begrenzungen, welche ein von manchen Autoren²⁸⁶ proklamiertes „Ausufern“ des Datenschutzes verhindern könnten. Zweifelsfrei steht den Verarbeiter:innen stets die Möglichkeit zur Verfügung, ihre Datenverarbeitungen einzuschränken bzw zu reduzieren. In der Praxis wird sich dies voraussichtlich für die diversen Anwendungen (vgl 5.2) dennoch als problematisch erweisen, auch wenn den Verarbeiter:innen durchaus die entsprechende Sensibilität für sensible Daten sowie Kreativität für den Umgang mit diesen zugetraut werden darf. Die von *Laimighofer* aufgezeigten Überlegungen können einen guten Anhaltspunkt für den Umgang mit pseudonymisierten personenbezogenen Daten darstellen, vermögen es jedoch nicht vollends für Bildaufnahmen zu überzeugen. Ein Begrenzungskriterium, wie es mit der „hinlänglichen Sicherheit“ beschrieben wird, kann in Kombination mit der Berücksichtigung des objektiven Risikopotentials der Verarbeitung zu einer gewissen Reduktion des Anwendungsbereichs beitragen. Trotz allem zeigt die hier dargestellte Aufarbeitung, dass schlussendlich die Judikatur und insbesondere die Gesetzgebung gefordert ist, klare Regelungen für die Verarbeitung von Bildaufnahmen zu schaffen. Die kürzlich ergangene Entscheidung des EuGH C-667/21 vom 21.12.2023 lässt allerdings auf eine „verarbeitungsfreundlichere“ Auslegung des Verarbeitungsverbots gemäß Art 9 Abs 1 DSGVO hoffen.

²⁸⁶ Vgl *Kienle*, LTZ 2023, 50 (67).

7 Literaturverzeichnis

- Assion Simon*, Die Entwicklung des Datenschutzrechts, NJW 2023, 2619
- Baumgartner Ulrich*, Bestimmung des Personenbezugs von Daten, ZD 2023, 399
- Bergauer Christian*, Die Einordnung von Bilddaten erkennbarer Personen im Datenschutzrecht. Eine Replik auf Knyrim, Bilddaten: immer sensibel?, jusIT 2016/103, 241
- Bergauer Christian*, Zur Rechtmäßigkeit der (Weiter-)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 2018/83, 231
- Bergauer Christian* in Jahnel Dietmar (Hrsg), Kommentar zur Datenschutz-Grundverordnung Art 4 Z 1 DSGVO (Jan Sramek 2021)
- Britz Thomas/Indenhuck Moritz/Langerhans Tom*, Die Verarbeitung „zufällig“ sensibler Daten, ZD 2021 (10), 559
- Brodil Wolfgang*, Datenschutz und Arbeitsrecht (LexisNexis ARD ORAC 2018)
- Deiters Gerhard*, EuGH zu Art. 9 Abs. 1 DSGVO: Sind nun „alle“ Daten besondere Kategorien personenbezogener Daten?, DSB 2022, 247
- Ernst Stefan* in Paal Boris/Pauly Daniel (Hrsg), DS-GVO BDSG³ Art 4 DSGVO (C. H. Beck Verlag 2021)
- Feiler Lukas /Forgó Nikolaus*, EU-DSGVO² § 12 DSG (Verlag Österreich 2022)
- Frenzel Eike Michael* in Paal Boris/Pauly Daniel (Hrsg), DS-GVO BDSG³ Art 9 DSGVO (C. H. Beck Verlag 2021)
- Gabauer Claudia*, Weite Auslegung der Begriffe „besondere Kategorien personenbezogener Daten“ und „sensible Daten“, RdM-LS 2023/63, 115
- Golland Alexander*, Kompetenz nationaler Wettbewerbsbehörden zur Feststellung eines Verstoßes gegen die DS-GVO, MMR 2023, 669
- Goricnik Wolfgang*, Unter welchen Voraussetzungen ist es datenschutzrechtlich zulässig, Fotos von Mitarbeitern digital zugänglich zu machen?, Dako 2023/14, 21
- Gosch Nicole*, Pseudonymisierung und Verschlüsselung sensibler Daten, jusIT 2019/39, 107
- Gosch Nicole*, Zur Reichweite der Klassifizierung sensibler Daten, jusIT 2022/76, 183
- Haidinger Viktoria/Löffler Michael*, Geheimhaltung: Zutrittskontrolle mittels Fotoabgleich, Dako 2023/12, 20
- Hense Peter*, Informationsaskese vs. Meta - Perspektiven des EuGH auf datengetriebene Praktiken in der modernen Gesellschaft, KuR 2023, 556
- Hessel Stefan/Dillschneider Jeanne*, Datenschutzrechtliche Herausforderungen beim Einsatz von Künstlicher Intelligenz, RD i 2023, 458
- Hödl Elisabeth* in Knyrim Rainer (Hrsg), DatKomm (2018) Art 4 DSGVO (Manz Stand 1.12.2018, rdb.at)
- Jahnel Dietmar*, EuGH: Dynamische IP-Adressen sind personenbezogene Daten, jusIT 2016/105, 252

Jahnel Dietmar, DSB: Bilddaten als nicht-sensible Daten, *jusIT* 2019/32 2019, 89

Jahnel Dietmar (Hrsg), Kommentar zur Datenschutz-Grundverordnung (DSGVO) Art 6 DSGVO (Jan Sramek 2021)

Jahnel Dietmar (Hrsg), Kommentar zur Datenschutz-Grundverordnung (DSGVO) Art 9 DSGVO (Jan Sramek 2021)

Kastelitz Markus/Hötzendorfer Walter/Tschohl Christof in *Knyrim Rainer* (Hrsg), *DatKomm* Art 9 DSGVO (Manz Stand 7.5.2020, rdb.at)

Kienle Thomas, Vorlage zur Vorabentscheidung – Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, *LTZ* 2023, 50

Knyrim Rainer, Bilddaten: immer sensibel?, *jusIT* 2016/102, 235

Kronegger Dieter, EuGH „Lindqvist“: Datenschutz im Internet, Medien und Recht 2004, 83

Lachmayer Konrad in *Knyrim* (Hrsg), *DatKomm* Art 1 DSGVO (Manz Stand 1.12.2018, rdb.at)

Laimighofer Albert, Was macht Fotos zu sensiblen Daten?, *jusIT* 2023, 102

Löw Manuel, „Bildnisschutz“: Absoluter Schutz vor unbefugtem Veröffentlichen von Lichtbildern?, *ZIIR* 2023, 142

Matejek Michael/Mäusezahl Steffen, Gewöhnliche vs. sensible personenbezogene Daten, *ZD* 2019, 551

Panic Stefan/Wolf Benedikt, Änderungen im Bereich der Bilddatenverarbeitung, *MR* 2020, 3

Pollirer Hans J./Weiss Ernst M/Knyrim Rainer/Haidinger Viktoria, DSG⁴ § 12 (Manz Stand 1.4.2019, rdb.at)

Schiff Alexander in *Ehmann Eugen/Selmayr Martin* (Hrsg), *Datenschutz-Grundverordnung² Art 9 DSGVO* (C. H. Beck Verlag 2018)

Schmidbauer Michael, Begriff und Verarbeitung sensibler Daten in der Judikatur des EuGH, *jusIT* 2023/32, 66

Schneider Jana/Schindler Stephan, Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten, *ZD* 2018, 463

Schulz Sebastian in *Gola Peter/Heckmann Dirk* (Hrsg), *Datenschutz-Grundverordnung - Bundesdatenschutzgesetz³ Art 9 DSGVO* (C. H. Beck Verlag 2022)

Sedef Arzu/Steiner Gerald, Datenverarbeitung, *Lexis Briefings <lexis360.at>* (Stand 21.7.2023)

Thiele Clemens, DSB: Zutrittskontrolle bei Skiliftanlagen, *jusIT* 2022/52, 116

Thiele Clemens, EuG: Zum relativen Personenbezug von Daten, *jusIT* 2023/65, 151

Thiele Clemens/Wagner Jessica, *EU-DSGVO: Umsetzung der DSGVO in der Personalpraxis* (Verlag Österreich 2019)

Thiele Clemens/Wagner Jessica (Hrsg), Praxiskommentar zum Datenschutzgesetz (DSG)² § 12 DSG
(Jan Sramek Verlag 2022)

Online-Quellen:

Artikel-29-Datenschutzgruppe, Advice paper on special categories of data (“sensitive data”), Ref Ares (2011) 444105, 4 <ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf> (22.01.2024)

EDSA, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.1, Rz 62ff
<edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_de.pdf> (22.01.2024)

EDSA, Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien“, Version 2.0, Rz 125 <edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_de_0.pdf> (22.01.2024)

<wko.at/branchen/information-consulting/werbung-marktkommunikation/fotografie-und-werbung.html>(12.11.2023)

Statistik Austria, IKT-EINSATZ IN UNTERNEHMEN (2021),
<statistik.at/fileadmin/publications/IKT_Unternehmen_2021.pdf> (28.07.2023)

<de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen> (28.07.2023)

8 Verzeichnis der Judikatur

EuGH:

EuGH 06.11.2003, C-101/01 (Lindqvist)

EuGH 01.08.2022, C-184/20 (Vyriausioji tarnybinės etikos komisija)

EuGH 8.12.2022, C-460/20 (Google)

EuGH 19. 10. 2016, C-582/14 (Breyer)

EuGH 04.06.2023, C-252/21 (Meta Platforms)

EuGH 21.12.2023, C-667/21 (MDK Nordrhein)

GA *PIKAMÄE* 09.12.2021, C-184/20

GA *RANTOS* 20.09.2022, C-252/21

BVwG:

BVwG 25.11.2019, W211 2210458-1

BVwG 20.11.2019, W256 2214855-1

BVwG 11.07.2023, W108 2250460-1

BVwG 21.04.2023, W245 2246467-1

BVwG 28.07.2023, W245 2245697-1

VfGH:

VfGH 14.12.2022, G 287/2022, G 288/2022

DSB:

DSB 07.06.2018, DSB-D202.207/0001-DSB/2018

DSB 21.01.2020, DSB 2020-0.013.649

DSB 21.06.2023, DSB 2022-0.930.971

DSB 23. 11. 2020, 2020-0.759.615

9 Anhang: Abstract

Die aktuelle Judikatur des EuGH betreffend die Verarbeitung von sensiblen Daten kann entscheidende Auswirkungen auf die Diskussion um die Einstufung von Bildaufnahmen als Verarbeitung besonderer Kategorien von personenbezogenen Daten haben.

Die bisher mehrheitlich in der deutschsprachigen Literatur vertretene Ansicht, dass subjektive Elemente, wie der Verarbeitungszweck des Verarbeiters, zu berücksichtigen sind, wurde durch den EuGH negiert. Gemäß dieser Entscheidung hat die Beurteilung nach objektiven Kriterien und unter Wahrung des hohen Schutzniveaus der DSGVO zu erfolgen. Aus den Erkenntnissen C-184/20 vom 01.08.2022 sowie C-252/21 vom 04.06.2023, lässt sich ein weites Verständnis des Art 9 Abs 1 DSGVO ableiten. Dies wird voraussichtlich auch große Auswirkungen auf die nationale Judikatur bzw Spruchpraxis der Datenschutzbehörde haben, welche bisher regelmäßig davon ausging, dass „normale“ Bildaufnahmen keine sensiblen Daten darstellen. Für die Praxis werden die bisherigen Verarbeitungen, insbesondere im Bereich von Bild- und Videoaufnahmen, sowie die Rechtsgrundlagen für diese zu überdenken sein. Dies insbesondere vor dem Hintergrund, dass der Spielraum für die Beschränkungen des weiten Anwendungsbereichs des Art 9 Abs 1 DSGVO bzw für „verarbeitungsfreundliche“ Auslegungsweisen äußerst gering ist. Aus der Anwendung des Kriteriums der „hinlänglichen Sicherheit“ sowie der Berücksichtigung des potenziellen Grundrechtseingriffs ergibt sich eine gewisse Reduktion dieses Anwendungsbereichs. Zusätzlich lässt der EuGH mit dem Erkenntnis C-667/21 vom 21.12.2023 jedoch auf eine „verarbeitungsfreundlichere“ Auslegung des Verarbeitungsverbots gemäß Art 9 Abs 1 DSGVO hoffen. Die weitere Judikatur sowie die Arbeit der Legislative ist allerdings abzuwarten, um ein endgültiges Ergebnis zur Kategorisierung von Bildaufnahmen feststellen zu können.

Abstract Englisch

The current judgement of the ECJ regarding the processing of sensitive data can have a decisive impact on the discussion about the classification of images as processing of special categories of personal data. The opinion previously held by the majority of German-speaking literature which stated that subjective elements such as the processing purpose of the processor must be taken into account has been rejected by the ECJ. The assessment must be made according to objective criteria and in compliance with the high level of protection provided by the GDPR. A broad understanding of Art. 9 para. 1 GDPR can be derived from the rulings C-184/20 of 1 August 2022 and C-252/21 of 4 June 2023. This is also likely to have a major impact on the national case law and decision-making practice of the data protection authority, which has so far regularly assumed that "normal" photographs do not represent sensitive data. In practice it will be necessary to rethink previous processing practices particularly in the field of image and video recordings as well as the legal basis

for these. This is particularly important regarding the potential for restrictions to the broad scope of application of Art. 9 para. 1 GDPR or for "processing-friendly" interpretations, which are extremely limited. However, the application of the technical term "hinlängliche Sicherheit" ("reasonable certainty") and the consideration of the potential interference with fundamental rights can offer a certain level of reduction. In addition, the ECJ's ruling C-667/21 of 21 December 2023 gives hope for a more "processing-friendly" interpretation of the processing prohibition pursuant to Art 9 para. 1 GDPR. However, further judicial decisions and the work of the legislature remain to be seen before a final result on the categorisation of image recordings can be determined.