Digitaler Zwilling im Metaverse – Eine rechtliche Untersuchung zum Authentifizierungsprozess

Jaouhara Zouagui, Peter Parycek

A. Einleitung

I. Metaverse: Verschmelzung von virtueller und physischer Welt

Der Begriff „Metaverse" stammt von Neal Stephenson aus dem Roman „Snow Crash" (1992) und beschreibt eine virtuelle 3D-Welt, in der Menschen[1] über Avatare interagieren. Trotz jahrzehntelanger Entwicklung gibt es keine einheitliche Definition, jedoch verbindet sie alle die Interaktion zwischen virtueller und physischer Welt.[2] Das Metaverse wird als nächste Iteration des Internets betrachtet,[3] dessen Entwicklung noch in den Anfängen steckt. Der Rat der Europäischen Union erwartet, dass es in 10 bis 15 Jahren etabliert sein wird.[4] Es soll Begegnungen in Echtzeit ermöglichen[5] und eine nachhaltige, zugängliche Erfahrung bieten, die mit der realen Welt verbunden ist. Reale physische Objekte werden ihre virtuellen Entsprechungen erhalten, wie z. B. Schuhe und Taschen, die im Metaverse vom Avatar des Nutzers getragen werden können.[6] Die reale und virtuelle Welt sowie öffentliche und private Netzwerke verschmelzen zu einer neuen Einheit mit eigenem Wirtschaftskreislauf. Charakteristisch für das Metaverse ist seine Interoperabilität: Nutzer sollen es in seiner ganzen Weite mittels eines einzigen Avatars oder einer einheitlichen digitalen Identität

1 Zur besseren Lesbarkeit wird im Verlauf der Arbeit das generische Maskulinum verwendet. Die Personenbezeichnungen beziehen sich jedoch auf alle Geschlechter.

2 *L. Xu,* Connecting Everyday Objects with the Metaverse: A Unified Recognition Framework, in: IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC) 2022, S. 401 (401 ff.).

3 *Kompetenzzentrum Öffentliche IT,* Metaversum, unter: https://www.oeffentliche-it.de/-/metaversum (alle Internetquellen dieses Beitrags wurden zuletzt aufgerufen am 12.10.2024).

4 *M. Martini/J. Botta*, Der Staat und das Metaversum, Zur Ordnungs- und Gestaltungsmacht im Internet von morgen, MMR 2023, 887 (888).

5 *M. Martini/J. Botta*, Metaversum (Fn. 4), 888.

6 *Bitkom e.V.,* Leitfaden Wegweiser in das Metaverse, Berlin 2022, S. 1 (7).

bereisen können.[7] Das Metaverse kann somit als virtueller Raum beschrieben werden, der durch unterschiedlich stark gewichtete Wesensmerkmale wie virtuelle Realität, virtuelle Vermögensgegenstände, digitale Identitäten und Interoperabilität geprägt ist.[8] Besonders entscheidend ist dabei die klare Zuordnung von virtuellen Vermögensgegenständen zu realen Personen mittels ihrer digitalen Identität.

II. Zugang und Interaktionen im Metaverse

Zugang zum Metaverse erhält man, wenn man sich bei einer Metaverse-Plattform als Nutzer registriert/anmeldet.[9] Diese Plattformen sind sowohl über einen Browser auf dem PC oder Smartphone als auch mit Virtual-Reality-Brillen zugänglich. Die Einsatzmöglichkeiten sind nahezu unbegrenzt und umfassen u. a. Spiele, virtuelle Treffen, Konsum und Kinobesuche.[10]

Personen agieren im Metaverse häufig über ihre digitalen Zwillinge, die sog. Avatare.[11] Diese repräsentieren die digitale Identität einer Person und können als Rechtssubjekte betrachtet werden.[12] Avatare werden physisch von Personen gesteuert und sind dadurch in der Lage, Willenserklärungen für den Erwerb von Dienstleistungen und Gütern in der virtuellen Welt abzugeben. Damit werden sie zu zentralen Zurechnungsobjekten im Metaverse.[13]

Die Erstellung digitaler Assets hat sich zu einer milliardenschweren Industrie entwickelt. Virtuelle Kleidung, Welten und Kunstwerke werden für echtes Geld gekauft.[14] In der Idealvorstellung des Metaverse können durch Avatare erworbene virtuelle Güter sowie reale Güter besessen und überallhin mitgenommen werden.[15] Die Vermögensgegenstände werden als Attribute elektronisch bestätigt und einer berechtigten Person (bzw.

7 *M. Martini/J. Botta*, Metaversum (Fn. 4), 888.
8 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Das Metaverse – eine rechtliche Einführung, RDI 2022, 323 (522).
9 *L. Bender-Paukens/S. Werry*, Datenschutz im Metaverse, Datenschutzrechtliche Herausforderungen im Zusammenhang mit der DSGVO, ZD 2023, 127 (128).
10 *M. Kaulartz/A. Schmid/F. Müller-Eising*, Metaverse (Fn. 8), 522.
11 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Metaverse (Fn. 8), 523.
12 *M. Kettermann/C. Böck*, § 6 Regulierung des Metaverse, in: H. Steege/C. Kuuya/M. Bagratuni (Hrsg.), Metaverse, Rechtshandbuch, Baden-Baden 2023, S. 114 (126).
13 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Metaverse (Fn. 8), 524 f.
14 *Bitkom e.V.,* Wegweiser (Fn. 6), S. 9.
15 *Bitkom e.V.,* Wegweiser (Fn. 6), S. 50.

deren Wallet) zugeordnet. Da an die Handlungen von Avataren rechtliche Anforderungen oder Konsequenzen geknüpft sein können, kann auch im virtuellen Raum ein Identifizierungsbedarf bestehen.[16] Nutzer sollten in der Lage sein, durch ihren Avatar Merkmale nachzuweisen, die mit ihrer Offline-Identität verbunden sind,[17] um beispielsweise im Metaverse beim Kauf von Vermögenswerten oder der Inanspruchnahme von Dienstleistungen notwendige Attribute datensparsam nachzuweisen. Im Folgenden wird eine geplante staatliche Lösung vorgestellt, um einem Avatar entsprechende Merkmale zuzuweisen.

B. Hauptteil

Bereits heute können Nutzer per Smartphone Zugang zum Metaverse erhalten und über ihren Avatar interagieren.

I. EUDI Wallet: Nutzung des Smartphones als Identifikationsinstrument im Metaverse

Eine verifizierbare Identität, die gleichzeitig den Datenschutz gewährleistet, ist ein entscheidender Baustein für ein zukünftiges dezentrales Metaverse.[18] Die im Frühjahr 2024 verabschiedete eIDAS-2.0-Verordnung (eIDAS 2.0) bildet den neuen rechtlichen Rahmen für die Gestaltung digitaler Identitäten in der Europäischen Union (EU). Sie bildet das Fundament für eines der wichtigsten Digitalisierungsvorhaben der EU und Deutschlands.[19] Nach der eIDAS 2.0 wird die sog. European Digital Identity Wallet (EUDI Wallet) eingeführt,[20] die für öffentliche Stellen sowie

16 *M. Lutz*, Sichere elektronische Identitäten und sichere Identifizierung im E-Government, in: D. Kipker/M. Barudi/K. Beucher (Hrsg.), Cybersecurity, München 2023, S. 632 (635).

17 *M. Zichichi/C. Bomprezzi/G. Sorrention/M. Palmirani*, Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland, in: Proceedings of the Fifth Distributed Ledger Technology Workshop (DLT) 2023, S. 1 (4 ff.).

18 *Bitkom e.V.,* Wegweiser (Fn. 6), S. 18.

19 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 - Die Brücke ins Digitale Zeitalter: Sichere digitale Identitäten als Schlüssel einer digitalen Gesellschaft, 2024, S. 1 (4).

20 *C. Busch*, § 16 Digitale Identitäten im Metaverse, in: H. Steege/K. Chibanguza/M. Bagratuni (Hrsg.), Metaverse Rechtshandbuch, Baden-Baden 2023, S. 293 (300 f.).

bestimmte privatwirtschaftliche Akteure verpflichtend wird. Dies betrifft auch sehr große Metaverse-Plattformbetreiber[21] gemäß Art. 33 Abs. 1 Digital Services Act (DSA), die die Wallet als Identifizierungsinstrument akzeptieren müssen.[22] Die nationale EUDI Wallet soll voraussichtlich Anfang 2027 verfügbar sein.[23]

1. Gestaltung digitaler Identitäten und Austausch verifizierter Daten im Lichte der EUDI Wallet

Die EUDI Wallet wird also künftig als zentrales Werkzeug für Bürger dienen, um auf private und öffentliche Onlinedienste zuzugreifen. Die EUDI Wallet auf dem Smartphone ermöglicht den verifizierten Austausch von selektiven Daten zwischen Behörden, Unternehmen und Bürgern. Diese Daten können sowohl Identitätsdaten (PID)[24] als auch Nachweise wie Eintrittskarten oder Meldebescheinigungen umfassen, die digital und verifizierbar übertragen werden können.[25] Mit der EUDI Wallet als staatliche Lösung können Benutzer ihren Avatar so mit verschiedenen Merkmalen bzw. Attributen ausstatten.[26]

a) Bestätigung von Merkmalen

Der eIDAS-Vorschlag und der Architektur-Referenzrahmen beschreiben die qualifizierte elektronische Bescheinigung von Attributen als generische, universelle elektronische Berechtigungsnachweise, die beliebige Benutzerdaten bestätigen. Qualifizierte elektronische Bestätigungen von Attributen

21 Art. 33 Abs. 1 DSA definiert Online-Plattformen mit einer durchschnittlichen monatlichen Zahl von mindestens 45 Millionen aktiven Nutzern in der EU als sehr große Online-Plattform. Erreicht eine Metaverse-Plattform diese Größe, unterliegt sie der Akzeptanzpflicht.

22 *C. Busch,* § 16 Digitale Identitäten (Fn. 20), S. 303.

23 *Bundesministerium des Innern und für Heimat,* Die eIDAS-Verordnung, unter: https://www.digitale-verwaltung.de/Webs/DV/DE/digitale-identitaeten/eidas-2-0/eidas-2-0-node.html.

24 Sog. Personal Identification Data.

25 *Bitkom e.V.,* eIDAS Leitfaden, Berlin Mai 2024, S. 1 (5 f.).

26 *M. Zichichi et. al.*, Protecting digital identity (Fn. 17), S. 4 ff.

(QEAAs) werden von qualifizierten Vertrauensdiensteanbietern bereitgestellt.[27]

Es wird zwischen elektronischen Bestätigungen von Attributen (EAAs) und QEAAs unterschieden: EAAs können aus staatlich autorisierten und „nicht-authentischen Quellen" stammen. EAAs aus staatlich autorisierten Registern gelten automatisch als QEAA und können in die Wallet ausgegeben werden. Attribute aus nicht staatlich autorisierten Quellen müssen von einem qualifizierten Vertrauensdiensteanbieter geprüft und validiert werden, um als QEAA anerkannt zu werden.[28] Diese (Q)EAAs werden zusammen mit den PID-Daten in der Wallet gespeichert,[29] um ein Merkmal im Kontext des Metaverse nachzuweisen.[30]

b) Einfluss auf die Modernisierung der Register

Die Umsetzung von eIDAS 2.0 als Rahmenwerk für digitale Identitäten wird auch die nationale Gesetzgebung, wie beispielsweise das Registermodernisierungsgesetz (RegMoG) und das Onlinezugangsgesetz (OZG) beeinflussen.[31] Der IT-Planungsrat beauftragte 2022 die Entwicklung eines Zielbildes für die Umsetzung der Registermodernisierung, das in das Nationale Once-Only-Technical-System (NOOTS) mündete.[32] Dieses System verfolgt das Once-Only-Prinzip (OOP), das es staatlichen Stellen ermöglicht, mit Einverständnis der Bürger bereits vorliegende Daten selbst (bei

27 *Bundesministerium des Innern und für Heimat,* Architecture Proposal for the German eIDAS Implementation, Version 2.2, 2014, S. 1 (40).

28 *Bundesdruckerei,* QEAA einfach erklärt: Bedeutung der Qualifizierten Elektronischen Attestierung von Attributen für die EUid-Wallet, unter: https://www.bundesdruckerei.de/de/innovation-hub/qeaa-einfach-erklaert#.

29 *Lissi GmbH*, EUDI-Wallet: Veranschaulichung der eIDAS-Rollen und Beziehungen, unter: https://www.lissi.id/de/blog/eudi-wallet-illustration-of-the-eidas-roles-and-relationships.

30 Vgl. *Die Europäische Kommission*, FAQ - EU Digital Identity Wallet, unter: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/FAQ.

31 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 4 f.

32 *Bundesverwaltungsamt,* Anbindungsleitfaden: Informationen für registerführende Stellen zur Anbindung an das Fachverfahren zum Identitätsdatenabruf (IDA), 2024, S. 9 (9).

anderen Behörden) abzurufen.[33] Das NOOTS-Gesamtsystem umfasst alle NOOTS-Komponenten, die für die Durchführung oder Nachvollziehbarkeit eines Nachweisabrufs notwendig sind[34] und formuliert Anschlussbedingungen.[35]

Die eIDAS 2.0 sieht die Öffnung der öffentlichen Register für den Nachweisabruf vor, während das OZG die Ausstellung von Attributsbescheinigungen für die Ausgestaltung der EUDI Wallet berücksichtigen muss. Daher ist es wichtig, die nationale Gesetzgebung mit der eIDAS 2.0 abzustimmen.[36] Derzeit sieht das RegMoG beispielsweise nur den Datenaustausch zwischen öffentlichen Stellen nach § 6 Identifikationsnummerngesetz (IDNrG) vor. Um eine effektive Nutzung der Register i.R.v. eIDAS 2.0 zu gewährleisten, sollten häufig angefragte Register zeitnah geöffnet und der gesetzliche Rahmen in den Fachgesetzten angepasst werden. Dies erfordert u. a. die Verfolgung des OOP, die Priorisierung wesentlicher Register für die geplanten Anwendungsfälle der EUDI Wallet sowie eine enge Verzahnung mit dem OZG.[37]

2. Neuer biometrischer Authentifizierungsprozess im Lichte der EUDI Wallet

Der Austausch von Identitätsdaten, bei dem auch staatliche Register einbezogen werden, ist eine zentrale Funktion der Wallet und eine wichtige Neuerung von eIDAS 2.0.[38] Die Authentifizierung des Identitätsinhabers bei jeder Vorlage der PID erfolgt auf Basis des deutschen elektronischen Identitätsnachweises (eID) als staatliche digitale Identität.[39] Die Verordnung macht die eID damit zum zentralen Bestandteil der Wallet auf dem Smartphone, die Personenidentifizierungsdaten auf hohem Vertrauensni-

33 *Bundesverwaltungsamt,* Nutzen der Registermodernisierung, unter: https://www.bva.bund.de/DE/Services/Behoerden/Verwaltungsdienstleistungen/Registermodernisierung/Ueberblick/ueberblick_node.html.
34 *Bundesministerium des Innern und für Heimat,* High-Level-Architecture (HLA), unter: https://bmi.usercontent.opencode.de/noots/AD-NOOTS-03_%2BHigh-Level-Architecture%2B_HLA_/.
35 *Bundesverwaltungsamt,* Anbindungsleitfaden (Fn. 32), S. 9.
36 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 4 f.
37 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 9.
38 Vgl. *Bitkom e.V.,* eIDAS Leitfaden (Fn. 25), S. 6.
39 *Bundesministerium des Innern und für Heimat,* Architecture Proposal (Fn. 27), S. 35.

veau bereitstellt.[40] Der Authentifizierungsprozess der eID-Funktion (auch als Online-Ausweisfunktion bekannt) spielt dabei eine entscheidende Rolle.

a) Authentifizierungsprozess

Die nationale eID ist die Online-Ausweisfunktion nach § 18 Personalausweisgesetz (PAuswG). Sie gewährleistet eine Identifizierung und basiert auf einer Zwei-Faktor-Authentifizierung gemäß Art. 8 Abs. 2 c eIDAS 2.0. Durch die Kombination von Ausweis (Besitz-Element) und PIN-Nummer (Wissens-Element) wird zwar eine hohe Sicherheit erreicht, jedoch ist die Benutzerfreundlichkeit eingeschränkt. Laut der eGovernment MONITOR Studie 2024 nutzten 2023 lediglich 14 % der Befragten den Online-Ausweis. 2024 stieg dieser Anteil auf 22 %.[41] Damit ist die eID trotzdem noch weit von einer flächendeckenden Nutzung entfernt. Dies hat verschiedene Gründe, darunter die wenig benutzerfreundliche Eingabe der sechsstelligen PIN.[42]

Der nachfolgende Beitrag befasst sich mit der Optimierung der Anwendungsfreundlichkeit der eID-Funktion durch den Wegfall der PIN-Eingabe für Anwendungszwecke der Smartphone EUDI Wallet. Wenn der Zugang zum Metaverse über ein Smartphone per EUDI Wallet erfolgt, könnte sich die Möglichkeit bieten, biometrische Daten zur Authentifizierung im Rahmen eines Touch-ID- oder Face-ID-Verfahrens zu nutzen, wodurch die PIN-Eingabe ersetzt wird. Für eine sichere Nutzerauthentifizierung mit hohem Vertrauensniveau sind mindestens zwei Authentifizierungsfaktoren aus verschiedenen Kategorien erforderlich.[43] Das Besitzelement wird durch den biometrischen Authentifizierungsfaktor ergänzt. Bei dieser Form der Authentifizierung muss ein Nutzer ein biometrisches Merkmal, wie einen Fingerabdruck oder ein Gesichtsbild, zur Verfügung stellen. Das System vergleicht dieses Merkmal mit einer registrierten Vorlage.[44] Nach § 12 eID-Karte-Gesetz (eIDKG) kann die eID aus einem elektronischen Speicher- und Verarbeitungsmedium in einem mobilen Endgerät erfolgen.

40 *Bundesdruckerei*, eIDAS 2.0: Alle Änderungen im Überblick 2023, unter: https://www.bundesdruckerei.de/de/innovation-hub/eidas/eidas-2-0#.

41 *Initiative D21 e.V./Technische Universität München,* eGovernment MONITOR 2024, 2024, S. 18 (19 f.).

42 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 3.

43 ABI L 2024/1183, 18.

44 *H. Zhong/C. Huang/X. Zhang/M.,* Metaverse CAN: Embracing Continuous, Active, and Non-intrusive Biometric Authentication, in: IEE Network, 2023, S. 67 (70).

§ 19 eIDKG schreibt jedoch vor, dass keine biometrischen Daten im eID-Karten-Register für die Online-Ausweisfunktion geführt werden.

Die freiwillige Online-Ausweisfunktion kann beispielsweise zur digitalen Kontoeröffnung im Finanzbereich[45] ohne die Nutzung biometrischer Daten verwendet werden. Der Einsatz von Biometrie im elektronischen Ausweisdokument dient nur der Verifikation des Ausweisinhabers bei einer hoheitlichen Identitätskontrolle. Dies ermöglicht eine einfachere Überprüfung, ob die Person, die den Ausweis vorlegt, tatsächlich der Inhaber ist. Beispielsweise können zwei Personen, die für das menschliche Auge nahezu identisch erscheinen, durch einen computerunterstützten Gesichtsvergleich bei einer Grenzkontrolle voneinander unterschieden werden.[46] Die folgende Tabelle 1 zeigt, welche Daten bisher bei den genannten Anwendungsbeispielen der eID verwendet werden.

45 Bsp. *Bundesministerium des Innern und für Heimat*, Anwendungen: ING Deutschland, unter: https://www.personalausweisportal.de/SharedDocs/anwendungen/Webs/PA/DE/Unternehmen/ing.html.

46 *Bundesamt für Sicherheit in der Informationstechnik*, Biometrie in elektronischen Ausweisdokumenten, unter: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Elektronische-Ausweisdokumente/Biometrie/biometrie_node.html.

Daten	Hoheitliche Identitätskontrolle	Online-Ausweisfunktion (freiwillig)
Familienname und Vornamen	+	+
Geburtsdatum und -ort	+	+
Anschrift und Postleitzahl	+	+
wenn angegeben: Ordens- bzw. Künstlername	+	+
wenn angegeben: Doktorgrad	+	+
Biometrische Daten		
digitales Lichtbild	+	–
digitale Fingerabdrücke	+	–
Weitere Angaben		
Seriennummer des Ausweises	+	–

Tabelle 1: Datenübertragung der Online-Ausweisfunktion.[47]

Lediglich im Chip des Personalausweises werden zwei Fingerabdrücke und das Lichtbild als biometrische Daten gespeichert, die als Vorlage dienen könnten. Die Fingerabdrücke werden ausschließlich für die Speicherung im Chip des Personalausweises erhoben. Spätestens wenn der Ausweis abgeholt wird, werden die Fingerabdrücke beim Hersteller und in der Personalausweisbehörde gelöscht.[48] Dann können nur die Behörden, die nach

47 *Bundesministerium des Innern und für Heimat,* Daten im Chip, unter: https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/der-personalausweis/daten-im-chip/daten-im-chip-node.html.

48 *Bundesministerium des Innern und für Heimat,* Ihr Personalausweis, unter: https://www.personalausweisportal.de/SharedDocs/downloads/Webs/PA/DE/informationsmaterial/flyer-broschueren/Broschuere_ihr_Personalausweis.pdf?__blob=publicationFile&v=23.

§ 16 PAuswG zur Identitätsfeststellung ermächtigt sind, die biometrischen Daten zu bestimmten Zwecken aus dem Chip auslesen.[49]

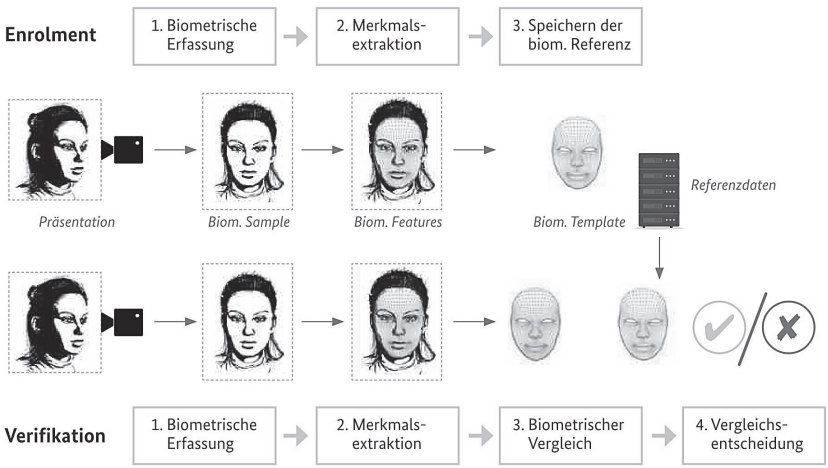

Abbildung 1: Prozessdarstellung von der Erfassung bis zur Vergleichsentscheidung in einem biometrischen System.[50]

Neben der Speicherung des Lichtbildes auf dem Chip des Personalausweises wird dieses jedoch auch im Personalausweisregister nach § 23 Abs. 3 PAuswG geführt.[51] Da lediglich über das Personalausweisregister auf das Lichtbild zugegriffen werden kann (Fingerabdrücke sind nicht verfügbar), fokussiert dieser Beitrag den biometrischen Datenabgleich des Lichtbildes für ein Face-ID-Verfahren aus dem Personalausweisregister, das bei den Personalausweisbehörden angesiedelt ist. Dieses Lichtbild dient als Referenz (Gesichtsprofil Template) für den biometrischen Datenabgleich nach Abbildung 1, um statt der PIN-Eingabe ein biometrisches Merkmal zur Authentifizierung i.R.d. EUDI Wallet-Lösung verifizieren zu lassen.

49 *Bundesministerium des Innern und für Heimat,* Daten im Chip (Fn. 47).

50 *Bundesamt für Sicherheit in der Informationstechnik,* Whitepaper 01 - Digitaler Verbraucherschutz: Bewertung des Usable Security und IT-Sicherheit biometrischer Verfahren in der Zwei-Faktor-Authentisierung, Bonn 2024, S. 1 (7).

51 Vgl. *G. Hornung,* Die digitale Identität, Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden 2005, S. 47 (51 f.).

b) Grundlegende Architektur der Registermodernisierung

Für den biometrischen Authentifizierungsprozess der eID ist vorgesehen, die NOOTS-Architektur für den Abruf von Nachweisen i.R.d. Registermodernisierung zu nutzen (s.o. B.I.1.b.). Eine Komponente des NOOTS ist das Identitätsmanagement (IDM) für Personen,[52] das gemäß § 1 IDNrG die Bereitstellung einer eindeutigen Identifikationsnummer (IDNr), auch bekannt als Steuer-ID, sowie weiterer personenbezogener Daten, den sog. Basisdaten nach § 4 Abs. 2 IDNrG, verantwortet. Folgende Daten werden als Basisdaten zugeordnet: IDNr, Familienname, frühere Namen, Vornamen, Doktorgrad, Tag und Ort der Geburt, Geschlecht, Staatsangehörigkeiten, gegenwärtige oder letzte bekannte Anschrift, Sterbetag, Tag des Einzugs und Auszugs.[53] Dies ist notwendig, um Personenverwechselungen bei den registerübergreifenden Datenübermittlungen zu verhindern.[54]

Technisch wird das IDM für Personen durch das Identitätsdatenabruf-Verfahren (IDA-Verfahren) des Bundesverwaltungsamts (BVA) umgesetzt, wie in Abbildung 2 dargestellt.[55] Neben der IDNr werden in der Steuer-ID-Datenbank vom Bundeszentralamt für Steuern (BZSt) die Basisdaten gespeichert, um die Zuordnung der IDNr zu einer natürlichen Person zu ermöglichen.[56] Die registerführenden Stellen des Bundes und der Länder integrieren die Steuer-ID in ihre Datenbestände und aktualisieren die Informationen, die den Basisdaten entsprechen (§ 2 Nr. 1 und 2 IDNrG).[57]

52 *Gesamtsteuerung Registermodernisierung,* Projekt „Gesamtsteuerung Registermodernisierung": Bericht zum Umsetzungsstand, 2022, S. 1 (7).
53 *Bundesverwaltungsamt,* Anbindungsleitfaden (Fn. 32), S. 26.
54 *J. Botta*, Der digitale Staat als gläserner Staat: Transparenz als Bedingung verfassungskonformer Registermodernisierung, Baden-Baden 2023, S. 27 (30).
55 *Bundesverwaltungsamt,* Anbindungsleitfaden (Fn. 32), S. 10.
56 *Finanzministerium Thüringen,* Vorhaben der Registermodernisierung, unter: https://registermodernisierung.thueringen.de/registermodernisierung-vorhaben-und-voraussetzungen.
57 *J. Botta*, Der digitale Staat (Fn. 54), S. 30.

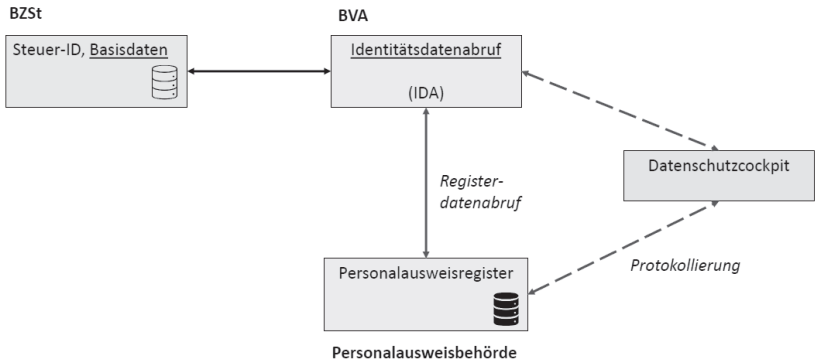

Abbildung 2: IDA-Verfahren am Beispiel der Anbindung des Personalausweisregisters.[58]

Um den Abruf der IDNr und der übrigen Basisdaten zu ermöglichen, müssen die dezentralen Register (in diesem Fall das Personalausweisregister der registerführenden Stelle) an das IDA-Verfahren angeschlossen werden,[59] damit das Lichtbild aus dem Personalausweisregister für den biometrischen Datenabgleich abgerufen werden kann. Das Datenschutzcockpit gemäß § 10 OZG ist eine IT-Komponente, die es betroffenen Personen ermöglicht, Informationen zu der entsprechenden Datenübermittlung zwischen den öffentlichen Stellen einzusehen (§ 10 Abs. 1 S. 1 OZG).[60]

Die folgende Abbildung 3 zeigt den Entwurf eines vereinfachten Prozessmodells zur Nutzung der Online-Ausweisfunktion mit der EUDI Wallet per Gesichtserkennungstechnologie, basierend auf dem NOOTS-Konzept.

58 Modifizierte Darstellung angelehnt an: *Finanzministerium Thüringen,* Vorhaben der Registermodernisierung (Fn. 56).

59 *KGSt,* Registermodernisierung, unter: https://www.kgst.de/registermodernisierung.

60 Im Datenschutzcockpit erhält die betroffene Person eine Übersicht über die Datenübermittlungen nach § 9 Abs. 1 IDNrG, bei denen ihre IDNr verwendet wurde (§ 10 Abs. 1 S. 2 OZG). Konkret kann die betroffene Person nachträglich die Protokolldaten gemäß § 9 IDNrG, einschließlich der übermittelten Inhaltsdaten und der Bestandsdaten der Register einsehen (§ 10 Abs. 2 S. 1 OZG) [*J. Botta*, Der digitale Staat (Fn. 54), S. 39 ff.].

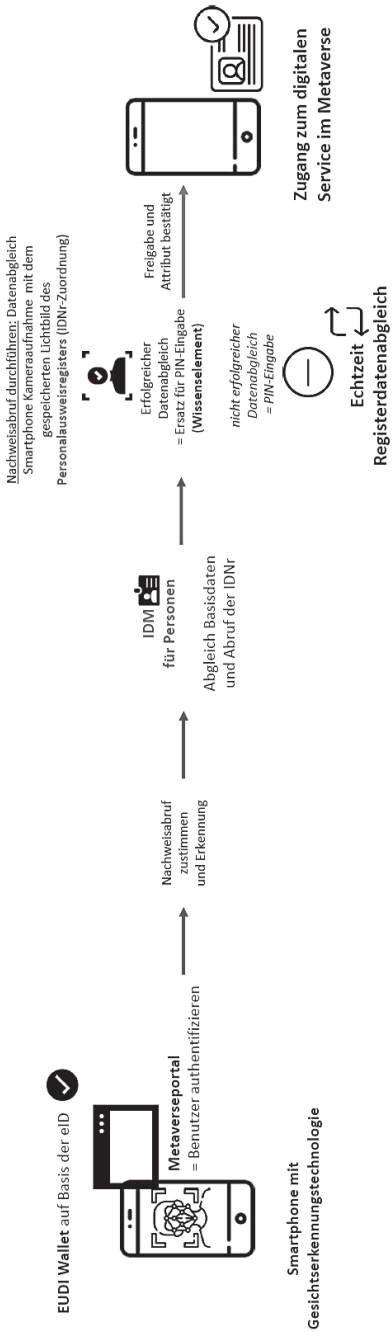

Abbildung 3: Vorgangsmodell zum biometrischen Authentifizierungsverfahren im Metaverse.[61]

Im Personalausweisregister wird das vom Smartphone übertragene Foto mit dem Personalausweisbild abgeglichen und die Übereinstimmung bestätigt. Mit dieser Bestätigung des biometrischen Attributs kann die PIN-Eingabe bei der Online-Ausweisfunktion entfallen. Die Vereinfachung des Authentifizierungsprozesses durch ein biometrisches Verfahren erhöht die Anwendungsfreundlichkeit bei der Inanspruchnahme digitaler Services im Metaverse. Dabei ist jedoch entscheidend, dass die Datenschutzstandards eingehalten werden.

3. Zwischenfazit

Mit der Einführung der EUDI Wallet wird eine sichere Online-Authentifizierung sowie die Verwaltung und gezielte Weitergabe von Identitätsdaten auch im Metaverse ermöglicht. Den Authentifizierungsprozess gilt es durch ein datenschutzkonformes biometrisches Verfahren zu vereinfachen, auf dessen rechtliche Grundlage im Weiteren eingegangen wird.

II. Datenschutzrechtliche Prüfung des biometrischen Authentifizierungsprozesses der EUDI Wallet

Es ist zu untersuchen, ob die grundrechtlichen Schranken beim automatisierten Datenabgleich mit dem Lichtbild aus dem Personalausweisregister nach § 23 Abs. 3 PAuswG zum Zwecke der Identifizierung per Online-Ausweisfunktion gewahrt werden können.

Das biometrische Lichtbild, das aus der Datenbank des Personalausweises abgerufen wird, hat zur Aufgabe, natürliche Personen anhand ihrer biometrischen personenbezogenen Daten zu identifizieren.[62] Für die Speicherung biometrischer Merkmale ist eine präzise Zweckbestimmung erforderlich.[63] § 14 PAuswG legt fest, unter welchen Voraussetzungen berechtigte Behörden und Stellen personenbezogene Daten aus dem Ausweis erheben und verwenden dürfen. Eine Nutzung biometrischer Daten für die eID-Funktion ist nach §§ 15 bis 20 PAuswG nicht vorgesehen (s.o. Abbil-

61 Eigene Darstellung.

62 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Metaverse (Fn. 8), 526.

63 *C. Golembiewski/T. Probst,* Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen, Kiel 2003, S. 1 (24).

dung 1). Eine eigene gesetzliche Grundlage für ein biometrisches Authentifizierungsverfahren besteht derzeit nicht.

Es wird daher geprüft, ob die Verwendung des Lichtbildes für den biometrischen Authentifizierungsprozess der eID-Funktion zumindest durch die Einwilligung der Nutzenden zulässig ist.

1. Prüfungsmaßstab der Verarbeitung personenbezogener Daten im Mehrebenensystem

Zur Klärung der Zulässigkeit der Einwilligung in die Verarbeitung des biometrischen Lichtbildes aus dem Personalausweisregister für die Online-Ausweisfunktion muss festgestellt werden, ob der grundrechtliche Prüfungsmaßstab nach Unions- oder nationalen Grundrechten bestimmt wird.

Der rechtliche Rahmen der Digitalisierung wird maßgeblich durch das Datenschutzrecht bestimmt, soweit es um die Verarbeitung personenbezogener Daten geht. Das europäische Primärrecht nennt zwei relevante Rechte für den Datenabgleich des Lichtbilds. Zum einen das in Art. 8 Abs. 1 Grundrechtecharta (GRCh) bzw. in Art. 16 Abs. 1 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV)[64] verankerte Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten[65] und zum anderen das Recht auf Achtung des Privat- und Familienlebens gemäß Art. 7 GRCh, welches seinen historischen Ursprung im beinahe wortgleichen Art. 8 der Europäischen Menschenrechtskonvention (EMRK)[66] findet.[67] Auf nationaler Ebene bildet das verfassungsrechtliche Fundament des Datenschutzrechts hauptsächlich das Recht auf informa-

64 Als grundrechtlicher Maßstab ist ausschließlich Art. 8 GRCh anzuwenden, während Art. 16 Abs. 1 AEUV lediglich eine deklaratorische Funktion hat [*H. Bretthauer* in: L. Specht/R. Mantz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 1. Aufl., München 2019, § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 37].

65 *D. Caliebe/I. Sommer,* Datenschutz in: H. Lühr/R. Jabkowski/S. Smentek (Hrsg.), Handbuch Digitale Verwaltung, Wiesbaden 2019, S. 225 (226).

66 Letztlich hat Art. 7 GRCh gemäß Art. 52 Abs. 3 GRCh die gleiche Bedeutung wie Art. 8 EMRK. Nach dem Willen der GRCh, einschließlich der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR), wird Art. 8 EMRK als Auslegungshilfe für Art. 7 GRCh genutzt (vgl. *Wissenschaftliche Dienste des Deutschen Bundestages*, Die Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta, WD 11 – 3000 – 12/11, S. 6).

67 ABI C 2007/303/02, 20.

tionelle Selbstbestimmung[68] als besondere Ausprägung des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

Art. 8 und Art. 7 GRCh, verfolgen weitestgehend den gleichen Zweck wie das nationale Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, nämlich den Schutz der Freiheit und der Selbstbestimmung durch den Schutz personenbezogener Daten. Somit stehen sich Art. 8 und Art. 7 GRCh als EU-Primärrecht und das Recht auf informationelle Selbstbestimmung als deutsches Grundrecht[69] gegenüber.

Die Anwendbarkeit der Grundrechtecharta wird durch Art. 51 Abs. 1 GRCh bestimmt. Nach Art. 51 Abs. 1 S. 1 Var. 2 GRCh sind die EU-Mitgliedstaaten und somit auch Deutschland verpflichtet, die GRCh zu beachten, wenn sie Unionsrecht durch nationale Stellen umsetzen.[70] Laut den Bundesverfassungsgericht (BVerfG)-Beschlüssen „Recht auf Vergessen I"[71] und „Recht auf Vergessen II"[72] vom 6.11.2019 hängt der grundrechtliche Prüfungsmaßstab davon ab, ob eine vollständige Vereinheitlichung eines Bereichs durch das Unionsrecht vorliegt.[73]

Regelt das Unionsrecht die Materie abschließend, wie z. B. bei einer Verordnung oder einer vollharmonisierenden Richtlinie, haben die Unionsgrundrechte Vorrang und sind grundsätzlich abschließend. Das BVerfG führt aus: „Bei der Anwendung unionsrechtlich vollständig vereinheitlichter Regelungen sind grundsätzlich nicht die deutschen Grundrechte, sondern allein die Unionsgrundrechte maßgeblich." […] Die Anwendung der Unionsgrundrechte ist hier eine Konsequenz der Übertragung von Hoheitsbefugnissen auf die EU nach Art. 23 Abs. 1 S. 2 GG. Wenn die Union im Rahmen dieser Befugnisse Regelungen schafft, die in der gesamten Union gelten und einheitlich angewendet werden sollen, muss auch der Grundrechtsschutz, der bei Anwendung dieser Regelungen gewährleistet

68 Bereits im Jahre 1983 hatte das BVerfG im Volkszählungsurteil [BVerfGE 65, 1] festgestellt, dass unter den Bedingungen der modernen Datenverarbeitung der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG umfasst ist und hieraus das Grundrecht auf informationelle Selbstbestimmung abgeleitet [*D.* Caliebe/I. Sommer, Datenschutz (Fn. 65), S. 226 f.].

69 *M. Desoi*, Intelligente Videoüberwachung, Wiesbaden 2018, S. 45 (59).

70 Zur Auslegung *M. Ruffert/F. Grischek/M. Schramm*, Europarecht im Examen – Die Grundrechte, JuS 2020, 1022 (1023 ff.).

71 BVerfG NJW 2020, 265 (300).

72 BVerfG NJW 2020, 265 (314).

73 *N. Klass*, Das Recht auf Vergessen und die Zeitlichkeit der Freiheit, ZUM 2020, 265 (273).

werden soll, einheitlich sein. Diesen Grundrechtsschutz gewährleistet die GRCh der EU. Die deutschen Grundrechte sind in diesen Fällen nicht anwendbar, da dies das Ziel der Rechtsvereinheitlichung konterkarieren würde. Das BVerfG leitet zudem eine Vermutungswirkung für eine „Mitgewährleistung" der Unionsgrundrechte bei Wahrung der nationalen Grundrechte her. Diese basiert auf dem gemeinsamen Fundament der allgemeinen Rechtsgrundsätze und der EMRK als gemeinsamer Auslegungsmaßstab für die GRCh, wie für die nationalen Grundrechte, in den Fällen des Art. 52 Abs. 3 GRCh.[74]

Seit dem 25.5.2018 gilt in der gesamten EU die Datenschutz-Grundverordnung (DSGVO) nach Art. 288 Abs. 2 AEUV, unmittelbar und in Deutschland[75] zusätzlich auch das neue Bundesdatenschutzgesetz (BDSG),[76] die der Ausgestaltung der Verarbeitung personenbezogener Daten als Authentifizierungsfaktoren i.R.d. eID-Funktion Rahmenbedingungen setzen.[77] Ermächtigungsgrundlage für die DSGVO zur Ausgestaltung der Artt. 8, 7 GRCh[78] ist Art. 16 Abs. 2 AEUV. Dadurch ist das Europäische Parlament und der Rat der EU ermächtigt, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten zu erlassen.[79] Die DSGVO gilt unmittelbarer in allen EU-Mitgliedstaaten. Für ihre Geltung braucht es keine Umwandlung in nationales Recht.[80]

Der europäische Gesetzgeber hat die DSGVO jedoch nicht als klassische Verordnung ausgestaltet.[81] Sie ermöglicht den Mitgliedstaaten, durch sog. Öffnungsklauseln nationalen Spielraum im Datenschutzrecht zu schaffen.[82] § 1 Abs. 5 BDSG stellt den Vorrang der unmittelbar geltenden Bestimmun-

74 *J. Kühling*, Das „Recht auf Vergessenwerden" vor dem BVerfG – November(r)evolution für die Grundrechtsarchitektur im Mehrebenensystem, NJW 2020, 275 (277).
75 *H. Bretthauer* (Fn. 64), § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 5.
76 *J. Schneider*, Datenschutz nach der EU-Datenschutz-Grundverordnung, München 2019, S. 46 (46).
77 Vgl. *M. Martini/M. Wenzel*, "Once only" versus "only once": Das Prinzip einmaliger Erfassung zwischen Zweckbindungs-grundsatz und Bürgerfreundlichkeit, DVBI 2017, 749 (751).
78 *J. Schneider*, Datenschutz (Fn. 76), S. 46.
79 EG 12 DSGVO.
80 EuGH Urt. v. 31.1.1978 – Rs. C-94/77, Rn. 22.
81 *J. Kühling/M. Martini*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im euro-päischen und deutschen Datenschutzrecht?, EuZW 2016, 448 (449).
82 *J. Kühling/M. Martini*, Datenschutz-Grundverordnung (Fn. 81), 448 f.

gen der Verordnung fest und berücksichtigt somit den Anwendungsvorrang des Unionsrechts. Das BDSG greift daher nur insoweit ein, als die Regelungen der DSGVO ergänzungsbedürftig (obligatorische Öffnungsklauseln) oder zumindest ergänzungsoffen (fakultative Öffnungsklauseln) sind.[83] Für die Bewertung, ob ein datenschutzrechtlich vollständig determinierter Bereich vorliegt, ist entscheidend, ob im konkreten Fall der einschlägigen Vorschriften eine Gestaltungsoffenheit anzunehmen ist, nicht jedoch eine allgemeine Betrachtung des Regelungsbereichs.[84]

Der nationale Gesetzgeber hat für die Verarbeitung besonders sensibler personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO (s.u. B.II.3.) die Öffnungsklauseln in Art. 9 Abs. 2 lit. b, g, h und i DSGVO genutzt und § 22 BDSG formuliert.[85] Diese Vorschriften sind jedoch nicht relevant, wenn es um die Einwilligung zur Verwendung des Lichtbildes für den biometrischen Authentifizierungsprozess der eID-Funktion geht, sondern konkretisieren beispielsweise die Verwendung besonders sensibler Daten in der Gesundheitsvorsorge. Im konkreten Fall der Einwilligung in die Verarbeitung besonders sensibler personenbezogener Daten im Zusammenhang mit dem biometrischen Authentifizierungsverfahren der eID ist die Datenverarbeitung durch die DSGVO vollständig harmonisiert, was bedeutet, dass die Prüfung ausschließlich anhand der Unionsgrundrechte und der DSGVO zu erfolgen hat.[86]

2. Unionale grundrechtliche Prüfung Artt. 8, 7 GRCh

Der Prüfungsmaßstab für die Einwilligung in den biometrischen Datenabgleich i.R.d. eID-Funktion richtet sich allein nach Artt. 8, 7 GRCh.

83 *J. Kühling/J. Raab* in: J. Kühling/B. Buchner (Hrsg.), DS-GVO BDSG, 4. Aufl., München 2024, Einführung Rn. 128.

84 BVerfGE 152, 216 (247).

85 *E. Frenzel* in: B. Paal/D. Pauly (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl., München 2021, Art. 9 DSGVO Rn. 50.

86 Vgl. zur Determinierung des Datenschutzrechts [*H. Gersdorf*, Unvereinbarkeit der Regelungen des GlüStV 2021-Entwurfs zur Limitdatei und Aktivitätsdatei mit Unionsgrundrechten und der DSGVO, ZfWG 2021, 19 (20 ff.)].

a) Persönlicher und sachlicher Schutzbereich

Ein Bürger, der die EUDI Wallet auf Basis der eID nutzt, wird als natürliche Person betrachtet und ist Träger von Grundrechten. Damit zählt er zu „jeder Person" gemäß den Artt. 8, 7 GRCh.

Der Schutz des Privatlebens in Art. 7 GRCh umfasst den Schutz der Privatsphäre.[87] Art. 8 GRCh schützt alle personenbezogenen Daten, also sämtliche Informationen über eine bestimmte oder bestimmbare natürliche Person.[88] Eine Einschränkung auf sensible Daten erfolgt hier nicht. Im Hinblick auf den Schutz eines Betroffenen vor einer biometrischen Datenverarbeitung im Kontext der eID bilden Art. 7 und 8 GRCh einen einheitlichen Schutzbereich.[89] Sie berücksichtigen auch die Achtung des Privatlebens bei der Verarbeitung personenbezogener Daten und entfalten daher bei der Auslegung der DSGVO ihre Wirkung.[90]

Das Lichtbild des Personalausweisregisters beinhaltet gemäß der Begriffsbestimmung aus Art. 4 Nr. 14 DSGVO biometrische Daten, welche personenbezogene Daten darstellen, die mit speziellen technischen Verfahren gewonnen werden und die eindeutige Identifizierung einer natürlichen Person ermöglichen oder bestätigen. Sie sind privat und nicht öffentlich. Die Verwendung dieser personenbezogenen Daten für das biometrische Authentifizierungsverfahren der eID eröffnet somit den Schutzbereich nach Artt. 8, 7 GRCh.

b) Grundrechtseingriff

Die Verarbeitung personenbezogener Daten i.R.d. biometrischen Authentifizierungsverfahrens für die EUDI Wallet könnte einen Eingriff in die Unionsgrundrechte nach Artt. 8, 7 GRCh darstellen.

In Achtung des Privatlebens[91] stellt die Verarbeitung personenbezogener Daten einen Eingriff in Artt. 8, 7 GRCh dar.[92] In der datenschutzrechtlichen

87 BVerfGE 152, 216 (255).
88 *H. Jarass* in: H. Jarass (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl., München 2021, Art. 8 Rn. 6.
89 BVerfGE 152, 216 (254).
90 *H. Jarass*, GrCh (Fn. 88), Art. 8 Rn. 7.
91 *H. Bretthauer* (Fn. 64), § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 10.
92 Vgl. *J. Kühling/J. Raab*, DS-GVO BDSG (Fn. 83), Art. 2 Rn. 28.

Terminologie umfasst die Verarbeitung sämtliche Aktivitäten – unabhängig davon, ob sie automatisiert durchgeführt werden oder nicht. Dazu zählen das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten, Bereitstellen in anderer Form, Abgleichen, Verknüpfen, Einschränken, Löschen oder Vernichten personenbezogener Daten. Der Verarbeitungsbegriff ist demnach weit ausgelegt.[93] Die Verwendung des biometrischen Lichtbildes für den Authentifizierungsprozess der eID ist als Eingriff in Art. 8, 7 GRCh zu werten, da ein automatisierter Datenabruf des im Personalausweisregister gespeicherten Lichtbildes für einen biometrischen Datenabgleich erfolgt.

c) Eingriffsausschluss

Nach Art. 8 Abs. 2 GRCh ist ein Eingriff in das Recht auf Schutz personenbezogener Daten nicht rechtswidrig, wenn der Eingriff auf einer gesetzlichen Grundlage beruht oder auch, wenn eine Einwilligung der betroffenen Person vorliegt.[94]

Die Einwilligung stellt gemäß Art. 8 Abs. 2 S. 1 GRCh einen grundrechtlichen Erlaubnistatbestand für die Verarbeitung dar. Sie bedeutet keinen Grundrechtsverzicht[95] und ist auch kein Rechtfertigungsgrund[96] für Grundrechtseingriffe, sondern hebt schon tatbestandlich das Verbot der Verarbeitung personenbezogener Daten auf.[97] Wenn der Bürger wirksam in die Verarbeitung seiner personenbezogenen Daten i.R.d. biometrischen Authentifizierungsverfahrens der eID eingewilligt hat, liegt damit kein Grundrechtseingriff vor.

---

93 *H. Bretthauer* (Fn. 64), § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 17.

94 *H. Jarass*, GrCh (Fn. 88), Art. 8 Rn. 10.

95 *G.* Robbers, Der Grundrechtsverzicht: Zum Grundsatz „volenti non fit iniuria" im Verfassungsrecht, JuS 1985, 925 (928).

96 Die dogmatische Einordnung der Einwilligung wurde bisher nur kursorisch erörtert. Sie kann entweder als Eingriffsausschluss oder als Rechtfertigungsgrund wirken. In jedem Fall ist die Datenverarbeitung aufgrund der Entscheidung des Betroffenen zulässig [siehe dazu ausführlich *H. Bretthauer* (Fn. 64), § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn. 18 und 59)]. Im vorliegenden Fall wird die Einwilligung mangels Verhältnismäßigkeitsprüfung als Eingriffsausschuss charakterisiert [Vgl. *H. Jarass*, GrCh (Fn. 88), Art. 8 Rn. 10].

97 Vgl. *B. Stemmer* in: A. Wolff/S. Brink (Hrsg.), BeckOK Datenschutzrecht, 41. Ed., 1.5.2022, Art. 7 Rn. 25.

Voraussetzung für eine wirksame Einwilligung des Betroffenen in die Datenverarbeitung ist, dass die Einwilligung in Kenntnis der Sachlage erfolgt. Die Einwilligung kann lediglich für einen bestimmten Zweck erteilt werden. Vor der Erteilung der Einwilligung muss dieser Zweck so genau wie möglich festgehalten werden, da der Ausschluss des Eingriffs nur dann gilt, wenn auch „Treu und Glauben" entsprochen wird. Daran fehlt es stets bei rechtswidrigen Zwecken. Diesbezüglich normiert die GRCh die Anforderungen im Einzelnen jedoch nicht.[98] In Ausgestaltung der Artt. 8, 7 GRCh formt die DSGVO den Erlaubnistatbestand der Einwilligung genauer aus.[99]

Es wird im Folgenden geprüft, ob die Rahmenbedingungen der DSGVO für eine wirksame Einwilligung eingehalten werden können. Erteilt der Bürger eine wirksame Einwilligung zur Verarbeitung seiner personenbezogenen Daten für den biometrischen Authentifizierungsprozess i.R.d. EUDI Wallet-Nutzung, entfällt ein Eingriff in die unionalen Grundrechte der Artt. 8, 7 GRCh.

3. Zulässigkeit der Datenverarbeitung nach Art. 9 Abs. 2 lit. a Hs. 1 DSGVO

Die DSGVO unterscheidet zwischen „personenbezogenen" und „besonders sensiblen Daten", welche nach Art. 9 DSGVO nur unter strengen Anforderungen verarbeitet werden dürfen. Das Lichtbild des Personalausweises wird mit seinen biometrischen Merkmalen (gemäß Begriffsbestimmung nach Art. 4 Nr. 14 DSGVO; s.o. B.II.2.a.) zur eindeutigen Identifizierung einer natürlichen Person genutzt. Bei den biometrischen Daten handelt es sich um eine besondere Kategorie personenbezogener Daten nach Art. 9 Abs. 1 DSGVO.[100]

Durch die Verarbeitung der Kategorie „besonders sensibler personenbezogener Daten" geht ein höheres Gefährdungspotenzial für den Persönlichkeitsschutz des Bürgers aus. In Art. 9 Abs. 1 DSGVO wurde zwar das generell geltende Verbotsprinzip[101] im Datenschutzrecht für besonders sensible

98 *H. Jarass*, GrCh (Fn. 88), Art. 8 Rn. 11.

99 *I. Conrad/M. Tinnefeld*, Die selbstbestimmte Einwilligung im europäischen Recht, ZD 2018, 391 (392).

100 *M. Kaulartz/A. Schmid/F. Müller-Eising,* Metaverse (Fn. 8*),* 526.

101 Art. 5 DSGVO enthält die Grundsätze für die Verarbeitung personenbezogener Daten und ist somit die zentrale Norm der DSGVO. Dem Grundsatz der Rechtmäßigkeit nach Art. 5 Abs. 1 lit. a Var. 1 DSGVO wird das „Verbotsprinzip" entnommen.

Daten wiederholt, damit wurden aber nur bestimmte Datenkategorien abschließend als besonders schutzbedürftig benannt[102] und klargestellt, dass die Verarbeitung der biometrischen Daten für die Online-Ausweisfunktion nur mit einem Ausnahmetatbestand des Art. 9 Abs. 2 DSGVO Rechtfertigung erfahren kann.[103] Von diesen Erlaubnistatbeständen muss zumindest einer verwirklicht sein, damit das Verbot nicht greift.[104] Hier normiert Art. 9 Abs. 2 lit. a Hs. 1 DSGVO auch die Einwilligung.

Für die Einwilligung hält dann Art. 4 Nr. 11 DSGVO eine Legaldefinition bereit. Danach ist eine Einwilligung jede freiwillige, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung. Diese kann in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung erfolgen, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung, der ihn betreffenden personenbezogenen Daten, einverstanden ist (EG 42 DSGVO).[105]

a) Problem der Freiwilligkeit beim Ungleichgewicht Staat und Bürger

Eine Wirksamkeitsvoraussetzung der Einwilligung ist die Freiwilligkeit nach Art. 7 Abs. 4 DSGVO. Zwischen Bürgern und dem staatlichen Anbieter der eID-Funktion besteht ein strukturelles Ungleichgewicht, da die Behörde als Hoheitsträger auftritt (EG 43 S. 1 DSGVO). Deshalb ist eine Einwilligung gegenüber einer Behörde in der Regel nicht freiwillig.[106] Die DSGVO will verhindern, dass Bürger durch die Machtasymmetrie zur Zu-

Dieses Prinzip meint ein Verbot der Datenverarbeitung mit Erlaubnisvorbehalt. [*R. Stenzel* in: S. Gierschman/K. Schlender/R. Stentzel/W. Veil-Buchholtz (Hrsg.), Datenschutzgrundverordnung, Köln 2018, Art. 5 Rn. 24].

102 *J. Botta*, Datenschutz bei E-Learning-Plattformen, Rechtliche Herausforderungen digitaler Hochschulbildung am Beispiel der Massive Open Online Courses (MOOCs), Baden-Baden 2020, S. 180 (181).

103 Vgl. *E. Frenzel*, DS-GVO BDSG (Fn. 85), Art. 9 DSGVO Rn. 18.

104 *P. Reimer*, Verwaltungsdatenschutzrecht, Das neue Recht für die behördliche Praxis, Baden-Baden 2019, Rn. 114.

105 *U. Dammann*, Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307 (308).

106 *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, DSGVO – BDSG Text und Erläuterungen, 2020, S. 1 (29).

stimmung gedrängt werden.[107] Eine solche coactus-volui-Struktur[108] überschattet die Einwilligung eines Bürgers in die Verarbeitung seiner besonders sensiblen personenbezogenen Daten für den Authentifizierungsprozess üblicherweise nicht.[109]

In Ausnahmefällen kann eine Einwilligung als Rechtsgrundlage dienen, wenn die Datenverarbeitung im Zusammenhang mit den Aufgaben der Behörde steht und den Betroffenen keine Nachteile bei Verweigerung entstehen. Die Bürger müssen frei entscheiden können, ob sie das Behörden-Angebot für die Online-Ausweisfunktion nutzen wollen oder nicht.[110] Die biometrische Authentifizierung ist bei der eID als zusätzliche Option neben der PIN-Eingabe vorgesehen, deren Nutzung dem Bürger freisteht. Dadurch wird kein strukturelles Ungleichgewicht zwischen Bürger und Behörde geschaffen. Für die freiwillige Einwilligung muss der Bürger auch die Tragweite seiner Erklärung verstehen.[111] Er muss wissen, welche Daten an wen und zu welchem Zweck übermittelt werden.[112] Art. 5 Abs. 1 lit. a Var. 3 DSGVO unterstützt dies durch das Transparenzprinzip, auf das im Folgenden eingegangen wird.

b) Das Transparenzprinzip i.R.d. Einwilligung

Personen können nur dann über ihre personenbezogenen Daten entscheiden, wenn sie auch selbst wissen, wer wann was über sie weiß und zudem, was der Verantwortliche mit ihren persönlichen Daten plant oder wie er sie bereits verarbeitet hat.[113] Zu dieser Absehbarkeit trägt das Transparenzprinzip nach Art. 5 Abs. 1 lit. a Var. 3 DSGVO bei. Dazu ergänzt EG 39 S. 3 DSGVO die Nachvollziehbarkeit. Alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten im Kontext des bio-

107 Ausführlicher *M. Peifer*, Die Datenschutz-Grundverordnung aus Sicht der öffentlichen Verwaltung, PinG 2016, 222 (226).
108 *N. Bethge*, Die verfassungsrechtliche Zulässigkeit des Grundrechtsverzichts, Hamburg 2014, S. 165 (165 ff.).
109 Vgl. *M. Martini/M. Wenzel*, "Once only" (Fn. 77), 753.
110 *M. Martini/M. Wenzel*, "Once only" (Fn. 77), 753.
111 *E. Ehmann* in: E. Ehmann/M. Helfrich (Hrsg.), EG-Datenschutzrichtlinie, Köln 1999, Art. 2 Rn. 69.
112 *E. Frenzel* (Fn. 85), Art. 49, Rn. 6.
113 *D. Caliebe/I. Sommer*, Betroffenenrechte: Transparenz als Werkzeug und Voraussetzung der informationellen Selbstbestimmung, in: R. Jabowski/H. Lühr/S. Smentek (Hrsg.), Handbuch Digitale Verwaltung, Wiesbaden 2018, S. 225 (234).

metrischen Authentifizierungsverfahrens der eID-Funktion sind demnach in leicht zugänglicher und verständlicher sowie in klarer und einfacher Sprache abzufassen. An diesen Willen des Unionsgesetzgebers muss sich auch das sog. Amtsdeutsch messen lassen.

c) Erfüllung der Betroffenenrechte

Überdies wird das Transparenzprinzip durch Artt. 12–15 DSGVO[114] hergestellt. Art. 12 DSGVO statuiert zunächst einen „allgemeinen Teil" für die Informationspflichten. Art. 13 DSGVO regelt die Informationspflichten bei Direkterhebung[115] und Art. 14 DSGVO die indirekte Erhebung[116] während Art. 15 DSGVO das Auskunftsrecht bestimmt. Dieses reagiert auf Informationsbegehren der betroffenen Personen.[117]

Die DSGVO normiert im Unterschied zum früheren deutschen Datenschutzrecht keinen Direkterhebungsgrundsatz,[118] der dazu verpflichte die Daten bei der betroffenen Person selbst zu erheben. Sie enthält auch diesbezüglich keine Öffnungsklausel.[119] Damit steht es dem biometrischen Authentifizierungsprozess frei, die Informationen aus dem Personalausweisregister zu nutzen, sofern der Pflicht nachgekommen wird, den Bürger über die Datenerhebung zu informieren (Art. 14 Abs. 2 DSGVO).[120]

Die oben genannten Betroffenenrechte sind bei der biometrischen Datenverarbeitung der eID-Funktion zu beachten.

---

114 Der nationale Gesetzgeber hat auf Grundlage der Öffnungsklausel des Art. 23 DSGVO die Betroffenenrecht nach Artt. 12–15 DSGVO nationalrechtlich mit §§ 29, 32, 33 und 34 BDSG ausgeformt. Diese haben jedoch im Rahmen dieser Arbeit keine Relevanz, da die normierten Ausnahmen für den biometrischen Datenabgleich des Authentifizierungsprozesses der Online-Ausweisfunktion in der Regel nicht einschlägig sind und daher an dieser Stelle nicht tiefer behandelt werden.

115 *D. Caliebe/I. Sommer*, Betroffenenrechte (Fn. 113), S. 235.

116 *D. Caliebe/I. Sommer*, Betroffenenrechte (Fn. 113), S. 236.

117 *D. Caliebe/I. Sommer*, Betroffenenrechte (Fn. 113), S. 234.

118 So auch *B. Buchner*, Die Einwilligung im Datenschutzrecht, DuD 2016, 155 (156).

119 *J. Kühling/M. Martini*, Die Datenschutz-Grundverordnung und das nationale Recht, Greifswald 2016, S. 301 (316).

120 *J. Kühling/M. Martini*, Datenschutz-Grundverordnung (Fn. 119), S. 316.

d) Entbündelungsgebot und Opt-in-Gebot bei Gestaltung der Einwilligung

Wenn die Verwaltung Daten auf der Grundlage einer Einwilligung verarbeiten will, muss sie „entbündelte" Einwilligungen zulassen. Das bedeutet, dass sie für verschiedene Verarbeitungsvorgänge, bei denen das biometrische Authentifizierungsverfahren Anwendung finden soll, auch verschiedene Erklärungen gestatten muss, statt den Bürgern eine pauschale Einwilligung abzuverlangen (EG 43 S. 2 DSGVO). Pauschale Einwilligungen sind oft nicht ausreichend konkret und nachvollziehbar. Grundrechtsschonender und im Lichte des Kopplungsverbots angezeigt (Art. 7 Abs. 4, EG 43 S. 2 DSGVO) ist hier ein differenzierendes Modell,[121] welches den Bürger bei jeder Nutzung des biometrischen Authentifizierungsprozesses auffordert, seine Einwilligung zu aktualisieren.

Da Art. 9 Abs. 2 lit. a Hs. 1 DSGVO nur eine ausdrückliche Einwilligung der betroffenen Person gestattet, ist nur eine Opt-in-Lösung zulässig.[122] Vorausgefüllte Kästchen (Opt-out) sind unzulässig.[123] Die Aufforderung zur Einwilligung beim biometrischen Authentifizierungsprozess muss zudem klar und knapp erfolgen (EG 32 S. 6 DSGVO).

e) Widerruf der Einwilligung

Die Einwilligung zum biometrischen Datenabgleich i.R.d. Online-Ausweisfunktion kann der Bürger zu jedem Zeitpunkt mit ex-nunc-Wirkung widerrufen (Artt. 7 Abs. 3 S. 1, Abs. 3 S. 2 DSGVO). Darüber muss der Bürger vor der Zustimmung zur Nutzung seiner Daten informiert werden (Art. 7 Abs. 3 S. 3 DSGVO). Die Widerrufsmöglichkeit darf auch nicht unsachgemäß (z. B. durch Zwang zur Angabe von Gründen) erschwert werden, sondern sie muss „so einfach wie die Erteilung der Einwilligung" gestaltet (Art. 7 Abs. 3 S. 4 DSGVO) sein.[124]

4. Zwischenfazit

Beim automatisierten Datenabgleich mit dem Lichtbild aus dem Personalausweisregister zur Authentifizierung per Online-Ausweisfunktion werden

121 *M. Martini/M. Wenzel*, "Once only" (Fn. 77), 753.
122 *J. Kühling/M. Martini*, Die Datenschutz-Grundverordnung (Fn. 119), S. 451.
123 *J. Kühling/M. Martini*, Die Datenschutz-Grundverordnung (Fn. 119), S. 451.
124 *M. Martini/M. Wenzel*, "Once only" (Fn. 77), 754.

biometrische Daten gemäß Art. 9 Abs. 1 DSGVO verarbeitet. Zur Wahrung der unionsgrundrechtlichen Schranken und zur rechtlichen Zulässigkeit der Verwendung des Lichtbildes im Authentifizierungsprozess ist mindestens die Einwilligung der Nutzenden nach Art. 9 Abs. 2 lit. a Hs. 1 DSGVO erforderlich und in angesicht der datenschutzrechtlichen Prüfung möglich.

C. Schluss

Das Metaverse stellt eine Verschmelzung der virtuellen und physischen Welt dar und wird als nächste Iteration des Internets betrachtet.[125] Die EU-Kommission plant, die digitale Kompetenz der Unionsbürger zu stärken und eine Governance für virtuelle Welten zu entwickeln.[126] Bis 2030 sollen auch sichere digitale Identitäten das Rückgrat einer vernetzten Gesellschaft bilden und den Zugang zu verschiedenen digitalen Diensten im Metaverse erleichtern.[127]

Angesichts der Fragmentierung des Marktes für Identitätsdienste und der aktuellen Umbrüche im Regulierungsrahmen für digitale Identitäten ist eine Prognose zur weiteren Entwicklung digitaler Identitäten im Metaverse schwierig. Voraussetzungen für die breite Akzeptanz digitaler Identitätslösungen wie der EUDI Wallet sind insbesondere eine im Einklang mit der Sicherheit stehende Nutzerfreundlichkeit und breite Einsatzmöglichkeiten. Entscheidend ist, diese teilweise im Widerstreit stehenden Zielsetzungen in einen sachgerechten Ausgleich einer staatlichen eID zu bringen.[128]

Auch wenn es seit der Einführung der eID-Karte keinen nennenswerten Sicherheitsvorfall gegeben hat,[129] zeigt das Beispiel der eID-Funktion, dass die komplexe Umsetzung eines hohen Sicherheitsniveaus die Nutzerakzeptanz beeinträchtigt. Je mehr Endnutzer den Identifizierungsdienst in Anspruch nehmen, desto attraktiver wird dieser für Drittanbieter und umgekehrt. Aus Sicht der Drittanbieter wird die Motivation zur Implementierung der eID durch die geringen Nutzungszahlen beeinträchtigt. Zudem besteht Optimierungsbedarf bei der organisatorischen, technischen und finanziellen Integration, was hohe Eintrittsbarrieren zur Folge hat. Orga-

125 *Kompetenzzentrum Öffentliche IT, Metaversum (Fn. 3).*
126 *M. Martini/J. Botta*, Metaversum (Fn. 4), 892.
127 *CDU/CSU-Fraktion im Deutschen Bundestag,* eIDAS 2.0 (Fn. 19), S. 2.
128 *Bundesministerium des Innern und für Heimat,* Architecture Proposal (Fn. 27), S. 35.
129 *Bundesministerium des Innern und für Heimat,* Architecture Proposal (Fn. 27), S. 35.

nisatorisch ist beispielsweise erforderlich, dass jeder Service beschrieben und beantragt wird. Auch der technische Integrationsaufwand ist erheblich, da die eID-Architektur den Betrieb eines eigenen ID-Servers oder einen Vertrag mit einem ID-Server-Betreiber voraussetzt. Die Kosten für den Betrieb des Servers sind intransparent und für den Dienstanbieter schwer kalkulierbar. Darüber hinaus bietet das anscheinend schwach ausgeprägte eID-Plattformmanagement keine detaillierten Informationen zu Kosten oder Entwicklungsperspektiven. Daher sind entscheidende Aspekte für die Zunahme von Onlinediensten in Verbindung mit der eID nur begrenzt vorhanden.[130] Hier könnte jedoch die in der eIDAS 2.0 vorgesehene Akzeptanzpflicht einen Beitrag leisten, da sich Drittanbieter trotz aller organisatorischen, technischen und finanziellen Herausforderungen der Implementierung der EUDI Wallet nicht entziehen können. Dadurch könnte die eID i.R.d. EUDI Wallet bei der Inanspruchnahme von Onlinediensten eine kritische Masse an Nutzern erreichen und somit auch im Metaverse eine wichtige Rolle spielen.[131]

Für die eID-nutzenden Onlinedienste trägt der im Beitrag dargestellte Ansatz des biometrischen Authentifizierungsverfahrens zur Benutzerfreundlichkeit und damit zur Erhöhung der Nutzerakzeptanz bei. Die datenschutzrechtliche Prüfung des biometrischen Authentifizierungsprozesses für die EUDI Wallet zeigt, dass beim automatisierten Datenabgleich mit dem Lichtbild aus dem Personalausweisregister strikte rechtliche Rahmenbedingungen eingehalten werden müssen. Biometrische Daten gelten gemäß Art. 9 Abs. 1 DSGVO als besonders schützenswert und ihre Verarbeitung erfordert mindestens eine explizite und informierte Einwilligung der Nutzenden nach Art. 9 Abs. 2 lit. a Hs. 1 DSGVO. Im Beitrag wurde dargelegt, dass die Einwilligung für die biometrische Authentifizierung sowohl datenschutz- als auch grundrechtskonform erfolgen kann. Sie muss freiwillig, transparent und jederzeit widerrufbar sein, um den hohen Anforderungen des Datenschutzes gerecht zu werden. Zusätzlich könnte eine Ermächtigungsgrundlage über eine verhältnismäßige Zweckänderung der Verwendung des Lichtbildes gegeben sein oder idealerweise eine eigene Rechtsgrundlage für die Nutzung des biometrischen Authentifizierungsverfahrens ausgestaltet werden. Um das Face-ID-Verfahren auch für Touch-ID-Verfahren zu erweitern, müssen die im Chip des Personalausweises

130 *P. Parycek*, Stellungnahme Digitale Identitäten, unter: https://www.bundestag.de/resource/blob/902144/218654a68c61fdb639c383f2fcb8fe70/Parycek.pdf, S. 3 (4 f.).

131 *C. Busch,* § 16 Digitale Identitäten (Fn. 20), S. 303.

erfassten Fingerabdrücke in das Personalausweisregister überführt werden. Dies gilt es in einem gesonderten rechtlichen Gutachten zu prüfen.

Die Speicherung des Iris-Scan für Ausweisdokumente wurde bereits früher für Authentifizierungsverfahren an Flughäfen diskutiert.[132] Mit der Verwendung von Virtual-Reality-Brillen eröffnet sich ein neuer Anwendungsfall. Obwohl der Zugang zum Metaverse über ein Smartphone erfolgen kann, lässt sich nur durch Virtuelle Realität (Virtual Reality, VR) vollständig in die computergenerierte Wirklichkeit des Metaverse eintauchen.[133] Daher sollte diese technologische Entwicklung auch in einen einfachen und sicheren Authentifizierungsprozess der eID-Funktion Berücksichtigung finden.

Um das Potenzial der staatlichen elektronischen Identität zu heben, müssen mit ihr auch langfristige und umfangreiche Investitionsentscheidungen sowie eine Vision für digitale Identitäten einhergehen, die in eine Strategie zur Umsetzung münden. Dazu muss die eIDAS 2.0 vollumfänglich und in allen Facetten in das OZG und die Registermodernisierung integriert werden.[134]

132 *DER SPIEGEL*, Biometrischer Reisepass kostet 59 Euro, v. 1.6.2005 unter: https://www.spiegel.de/reise/aktuell/epass-biometrischer-reisepass-kostet-59-euro-a-358564.html.

133 Vgl. *Bitkom e.V.,* Wegweiser (Fn. 6), S. 14.

134 *Bitkom e.V.,* eIDAS Leitfaden (Fn. 25), S. 13 f.