Konferenz der unabhängigen Datenschutzaufsichtsbehörden
des Bundes und der Länder

Positionspapier zur biometrischen Analyse

Version 1.0, Stand: 3. April 2019

Beschlossen von der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. und 4. April 2019 gegen die Stimmen Bayerns und Baden-Württembergs.

Inhaltsverzeichnis

1 Ziel des Positionspapiers 4
2 Grundlagen der biometrischen Erkennung 4
2.1 Begriffsbestimmungen 4
2.2 Funktionsweise der biometrischen Erkennung 6
2.2.1 Allgemeine Beschreibung 6
2.2.2 Enrolment 7
2.2.3 Prüfung auf Übereinstimmung 7
2.2.4 Widerstand gegen Verfälschungen 8
3 Systeme zur Erfassung biometrischer Charakteristika 8
3.1 Erfassung biometrischer Charakteristika 8
3.1.1 Fingerabdruck/Finger-Bild 8
3.1.2 Iris 9
3.1.3 Netzhaut (Retina) 9
3.1.4 Gesicht 10
3.1.5 Handgeometrie 10
3.1.6 Venenmuster 10
4 Biometrische Sensoren 11
4.1 Videokameras 11
4.2 Infrarotkameras 12
4.3 Fingerabdruckleser 13
4.4 Handgeometrieleser 13
4.5 Irisscanner 14
4.6 Retinascanner 14
5 Sammlung möglicher Einsatzszenarien („Use Cases“) 15
5.1 Übersicht über Einsatzszenarien 15
5.2 Klassifikation der Szenarien nach technischen und funktionalen Aspekten 15
5.2.1 Kooperative biometrische Verifikation 15
5.2.2 Nicht-kooperative biometrische Erkennung 15
5.2.3 Zuordnung zu Gruppen 16
5.2.4 Profilbildung, Verkettung 16
5.2.5 Verhaltenserkennung 16
5.3 Betrachtung der Szenarien nach Zwecken im datenschutzrechtlichen Sinn 16
5.3.1 Hoheitliche Authentisierungsverfahren 16
5.3.2 Staatliche Identifikationsverfahren 16
5.3.3 Zutrittskontrolle 16
5.3.4 Zugangskontrolle 16
5.3.5 Werbung, Marketing 17
5.3.6 Reichweitenmessung von Werbung 17
5.3.7 Beobachtung, Überwachung 17
5.3.8 Mensch-Maschine-Interaktion, Steuerung 17
6 Rechtliche Bewertung 18
6.1 Begriff der biometrischen Daten nach Art. 4 Nr. 14 DS-GVO 18
6.1.1 Personenbezogene Daten 18
6.1.2 Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person 19
6.1.3 Daten, die die eindeutige Identifizierung einer natürlichen Person ermöglichen oder bestätigen 19
6.1.4 Mit speziellen technischen Verfahren gewonnene Daten 19
6.1.5 Verhältnis zum Begriff der biometrischen Daten nach ISO/IEC JTC SC37 19
6.1.6 Beispiele für biometrische Daten gemäß Art. 4 Nr. 14 DS-GVO 20
6.2 Voraussetzungen des Art. 9 DS-GVO 21
6.2.1 Grundsätze 21
6.2.2 Ausgewählte Ausnahmetatbestände des Art. 9 Abs. 2 DS-GVO 22
6.3 Anwendung des Art. 6 Abs. 1 DS-GVO 23
6.3.1 Einwilligung in die Datenverarbeitung gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO 24
6.3.2 Erforderlichkeit zur Erfüllung eines Vertrages oder eines vorvertraglichen Verhältnisses gem. Art. 6 Abs. 1 S. 1 lit. b DS-GVO 24
6.3.3 Erforderlichkeit zur Wahrung der berechtigten Interessen des Verantwortlichen gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO 24

6.4 Juristische Bewertung anhand ausgewählter Anwendungsfälle 26
6.4.1 Fall 1: Bezahlung des Schulessens mit Hilfe des Fingerabdrucks 26
6.4.2 Fall 2: Zugang zu Firmenräumen mit Hilfe des Fingerabdrucks 26
6.4.3 Fall 3: Biometrischer Lichtbildabgleich durch Skiliftbetreiber 27
6.4.4 Fall 4: Zutrittskontrolle mit Handvenenscan für Flughafenmitarbeiter 27
6.4.5 Fall 5: Zielgerichtete Außenwerbung durch biometrische Gesichtsanalyse 28
6.4.6 Fall 6: Zugangskontrolle auf Kreuzfahrtschiff 29
6.4.7 Fall 7: Videokamera in Juweliergeschäft 30
6.4.8 Fall 8: VIP-Gast-Erkennung in Hotels 31
7 Auswahl von Maßnahmen und Schlussfolgerungen für die Verfahrensgestaltung 31
7.1 Modell und Grundannahmen 31
7.1.1 Methodik 31
7.1.2 Systemaufbau 32
7.1.3 Überblick über die für biometrische Systeme typischen Verarbeitungen 33
7.2 Risiken 34
7.3 Maßnahmen 35
7.4 Restrisiko 35

1 Ziel des Positionspapiers

Der Einsatz moderner optisch-elektronischer Verfahren ist ein weiterer Baustein für eine immer umfassendere Profilbildung von Personen im Alltag. Anhand von Videoaufnahmen und der Auswertung des Gesichts einer Person können deren Alter und Geschlecht recht zuverlässig bestimmt werden. Durch Analyse der Mimik sind zusätzlich auch Rückschlüsse auf die Gefühlslage eines Menschen möglich (Emotional Decoding). All dies kann technisch ohne Wissen und Einverständnis der Betroffenen erfolgen. Derartige Verfahren werden beispielsweise verwendet, um die Wirksamkeit von Werbung zu messen und genauer auf die gewünschten Zielgruppen zuschneiden zu können.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ damit beauftragt, sich gemeinsam mit dem Arbeitskreis „Videoüberwachung“ mit dem Thema Verarbeitung von Daten durch Sensorik und Videotechnik und deren datenschutzrechtliche Einordnung zu befassen. Ziel ist es, die Leistungsfähigkeit von biometrischen Sensoren einschließlich Videokameras und der dazu gehörigen Verarbeitungssysteme zu ermitteln, sowie Verarbeitungsziele und -prozesse zu beschreiben. Anschließend werden diese Elemente rechtlich bewertet und Empfehlungen zur Gestaltung von Verfahren abgeleitet.

2 Grundlagen der biometrischen Erkennung

2.1 Begriffsbestimmungen

Die Begriffe und Definitionen sind Übersetzungen aus dem ISO/IEC JTC SC37 Harmonized Biometric Vocabulary (HBV), wie es in der SC37 Working Group 1 für den internationalen Standard ISO/IEC 2382-37 erarbeitet wurde.

Anonymisierter biometrischer Datensatz
Biometrischer Datensatz, der bewusst von personenbezogenen Metadaten entkoppelt wurde

Betroffene Person
Individuum, dessen individualisierte biometrische Daten sich innerhalb des biometrischen System befinden

Biometrische Anwendungs-Datenbank
Datenbank aus biometrischen Daten und zugeordneten Metadaten, die durch den Betrieb einer biometrischen Anwendung erzeugt wurden und diese unterstützen sollen

Biometrisches Charakteristikum
Biologisches oder verhaltensabhängiges Charakteristikum eines Individuums, von welchem sich zur Unterscheidung verwendbare, reproduzierbare biometrische Merkmale ableiten lassen, die zum Zwecke der biometrischen Erkennung einsetzbar sind

Biometrische Daten[1]
Biometrisches Sample oder Ansammlung biometrischer Samples in jeder Verarbeitungsstufe, biometrische Referenzen, biometrische Probe, biometrisches Merkmal oder biometrische Eigenschaften

Biometrisches Enrolment
Vorgang der Erzeugung und Speicherung eines biometrischen Enrolmentdatensatzes in Übereinstimmung mit den Enrolmentregeln

Biometrische Enrolmentdatenbank
Datenbank aus biometrischen Enrolmentdatensätzen[2]

[1] Die Definition weicht von der Begriffsbestimmung aus Art 4 Ziffer 14 DS-GVO ab; siehe auch Abschnitt 6.1 Begriff der biometrischen Daten nach Art. 4 Nr. 14 DS-GVO. Art 14. Ziffer 14 lautet: „Biometrische Daten“ *(sind)* mit speziellen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

[2] Eine Datenbank mit biometrischen Daten, die nicht einer betroffenen Person zugeordnet werden können, ist eine biometrische Datenbank, aber keine biometrische Enrolmentdatenbank.

Biometrischer Enrolmentdatensatz
Datensatz, der sich auf eine betroffene Person bezieht, nichtbiometrische Daten enthält und mit einem biometrischen Referenz-Identifikator assoziiert ist

Biometrisches Erfassungsgerät
Gerät, das in der Lage ist, aus einem biometrischen Charakteristikum ein Signal zu sammeln und in ein erfasstes biometrisches Sample zu konvertieren

Biometrisches Erfassungsteilsystem
biometrisches Erfassungsgerät(e) und zugehörige Teilprozesse, die für die Durchführung eines biometrischen Erfassungsprozesses notwendig sind

Biometrische Erkennung
Automatisierte Erkennung von Individuen anhand ihrer verhaltensbezogenen und biologischen Charakteristika

Biometrische Identifikation
Prozess um bei der Suche in einer biometrischen Enrolmentdatenbank den Identifikator einer biometrischen Referenz, der einem einzigen Individuum zugeordnet werden kann, zu finden

Biometrische Verifikation[3]
Prozess, eine biometrische Behauptung durch einen biometrischen Vergleich zu bestätigen

Biometrisches Merkmal
Zahlen oder Kennzeichen, die aus einem biometrischen Sample extrahiert wurden und zum Vergleich verwendet werden

Biometrische Merkmalsextraktion
Auf ein biometrisches Sample angewendeter Prozess mit dem Ziel, Zahlen und markante Kennzeichen wiederholbar zu isolieren und auszugeben, die mit anderen Zahlen und markanten Kennzeichen, die aus anderen biometrischen Samples gewonnen wurden, vergleichbar sind.

Biometrische Probe
Biometrische Samples oder biometrische Merkmale, die als Eingabe zu einem Algorithmus zum Vergleich mit einer biometrischen Referenz dienen

Biometrische Referenz
ein oder mehrere gespeicherte biometrische Samples, biometrische Templates oder biometrische Modelle, die einer betroffenen Person zugeordnet wurden und als Objekt zum biometrischen Vergleich verwendet werden

Biometrische Referenz-Datenbank
Datenbank mit biometrischen Referenzdatensätzen

Biometrisches Sample
Analoge oder digitale Repräsentation biometrischer Charakteristika vor der biometrischen Merkmalsextraktion

---

Eine biometrische Enrolmentdatenbank kann die biometrische Referenzdatenbank enthalten, muss aber nicht. Eine Trennung der Datenbanken kann aus Gründen der Sicherheit, des Datenschutzes, der Rechtslage, der Systemarchitektur oder der Erkennungsleistung erforderlich sein.

[3] Der Begriff der *biometrischen Authentifikation* wurde im Prozess der Standardisierung von ISO/IEC 2382-37 als veraltet abgelehnt.
Der Begriff *Authentisierung* wird in diesem Papier deshalb so verwendet, wie vom Bundesamt in der Sicherheit der Informationstechnik im Glossar des IT-Grundschutz-Kompendiums definiert (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html):
„Authentisierung bezeichnet den Nachweis oder die Überprüfung der Authentizität. Die Authentisierung einer Identität kann u. a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen.
Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen."

Biometrisches System
System zum Zwecke der biometrischen Erkennung von Individuen anhand ihrer verhaltensbezogenen und biologischen Charakteristika[4]

Biometrisches Identifikationssystem
System zum Zwecke der biometrischen Identifikation

Biometrisches Template (Synonym: Referenz-Merkmalsvektor)
Menge von gespeicherten biometrischen Merkmalen, die direkt vergleichbar zu den biometrischen Merkmalen einer biometrischen Probe sind.

Enrolen (registrieren)
Erstellen und Speichern eines biometrischen Enrolmentdatensatzes in Übereinstimmung mit einer biometrischen Enrolmentregel

Nichtauthentische Person
Biometrisch subversive zu erfassende betroffene Person, die versucht mit der biometrischen Referenz einer anderen Person Übereinstimmung zu erlangen

Nicht identifizierte biometrische Daten
biometrische Daten, deren betroffene Person derzeit nicht bekannt ist

Präsentation, bewusste
Präsentation unter dem Bewusstsein der zu erfassenden betroffenen Person

Präsentation, kooperative
Präsentation durch eine kooperative zu erfassende betroffene Person

Präsentation, indifferente
Präsentation, bei der die zu erfassende betroffene Person sich des durchgeführten biometrischen Erfassungsprozesses nicht bewusst ist

Präsentation, unkooperative
Präsentation einer unkooperativen zu erfassenden betroffenen Person

Verdecker einer Identität
Subversive zu erfassende betroffene Person, die versucht, sich einer Übereinstimmungsentscheidung mit der eigenen biometrischen Referenz zu entziehen

Vergleich
Schätzung, Berechnung oder Messung der Ähnlichkeit oder Unterschiedlichkeit zwischen der biometrischen Probe und biometrischen Referenzen

2.2 Funktionsweise der biometrischen Erkennung

2.2.1 Allgemeine Beschreibung

Verfahren zur biometrischen Erkennung sind immer Teil eines umfassenderen biometrischen Systems. Mit der biometrischen Erkennung soll festgestellt werden, ob ein gegenüber einem biometrischen Erfassungssystem präsentiertes biometrisches Charakteristikum mit einer bekannten biometrischen Referenz übereinstimmt. Beispiele für biometrische Systeme sind in Kapitel 5 dargestellt. Dabei kann festgestellt werden, ob eine Person bekannt ist, d.h. ob biometrische Daten von ihr vorliegen, oder ob sogar weitergehende Daten wie Name, Adresse usw. bekannt sind. Abhängig vom Ergebnis der Prüfung wird dann in dem System fortgefahren.

Bei der biometrischen Erkennung können drei Phasen unterschieden werden:

In der initialen Phase werden die biometrischen Charakteristika erstmalig erfasst, Merkmale berechnet und Referenzen gespeichert. Im Falle eines Enrolments werden diese biometrischen Daten mit weiteren Daten verknüpft.

[4] Ein biometrisches System enthält biometrische und nichtbiometrische Komponenten.

Das eigentliche (Wieder-) Erkennen findet im Rahmen des biometrischen Systems statt, wenn nach erneutem Erfassen der biometrischen Charakteristika die Merkmale errechnet werden und im Vergleich mit den vorhandenen Referenzdaten festgestellt wird, ob die Person bekannt ist.

Die abschließende Phase ist das Löschen des biometrischen Merkmals und der zugehörigen Daten.

2.2.2 Enrolment

Grundsätzlich müssen als Ergebnis der ersten Phase die Referenzwerte gewonnen werden. Dies geschieht, indem biometrische Samples gewonnen sowie Merkmale errechnet werden, die bei einem Enrolment um weitere Daten ergänzt und dann in einer Referenzdatenbank gespeichert werden.

Üblicherweise wird in dieser Phase einem Erfassungsgerät (vgl. hierzu Abschnitt 3) ein zu einer Person gehörendes biometrisches Charakteristikum präsentiert. Daraus wird ein Sample oder ein Template generiert und in einer dezentralen Datenbank, beispielsweise dem Zutrittskontrollsystem der Niederlassung eines Verantwortlichen, einer zentralen Datenbank eines Verantwortlichen oder sogar übergreifend für mehrere Verantwortliche, wie im Bereich der Polizei, gespeichert. Weiterhin gibt es Systeme, bei denen die biometrischen Daten auf einem Datenträger (Chipkarte) gespeichert werden, der sich im Besitz der betroffenen Person befindet. Zusätzlich zu den biometrischen Daten werden noch Angaben zu der Person gespeichert. Bei Reisedokumenten wird als Sample ein Bild des Fingerabdrucks erstellt und dieses Bild wird (signiert) auf einem Chip des Dokuments gespeichert. Es gibt auch Entwicklungen, Templates zusätzlich zu einer reinen Zugriffskontrolle dergestalt zu schützen, dass sie nur in einem bestimmten System genutzt werden können (Biometric Template Protection).

Der Umfang der Daten, die zur Person gespeichert werden, kann abhängig von der Anwendung erheblich voneinander abweichen; siehe hierzu die verschiedenen Szenarien aus Kapitel 5.

Beim Enrolment kann es Fehler geben, die als FTE (Failure to Enrol Rate) bezeichnet werden; beispielsweise gibt es beim biometrischen Merkmal „Fingerabdruck“ Personen, deren Fingerabdrücke nicht genug ausgeprägt sind und daher nicht erfasst werden können.

Unabhängig von diesen sehr technischen Aspekten ist auch relevant, ob das Erfassen der Daten ohne Wissen des Betroffenen (wie etwa bei der Suche nach Straftätern, von denen nur ein biometrisches Merkmal bekannt ist), mit Wissen (wie bei einem Hinweis auf die Nutzung von Videotechnik) oder durch eine bewusste Präsentation des Betroffenen (wie bei Zutrittskontrollsystemen) stattfindet.

2.2.3 Prüfung auf Übereinstimmung

Nach der Erfassung, in der Regel also dem Enrolment, stehen die Referenzwerte zur Verfügung. Wenn im Rahmen des biometrischen Systems einem Erfassungsgerät ein biometrisches Charakteristikum präsentiert wird, werden daraus die Merkmale generiert. Diese werden mit den Merkmalen verglichen, die sich aus den Daten der Referenzdatenbank bzw. aus der vorgelegten Chipkarte ergeben. Das Ergebnis des Vergleichs wird in Form eines Prozentsatzes ausgegeben.

Es muss daher bei der Konfiguration des Verfahrens ein Schwellwert festgelegt worden sein, ab dem eine Übereinstimmung zwischen den Referenzen und dem gerade errechneten Wert angenommen wird. In Folge dieser systemisch bedingten Unschärfe gibt es Fälle, in denen eine Übereinstimmung angenommen wird, obwohl sie nicht vorlag (FAR: False Acceptance Rate) und es gibt Fälle, in denen eine Person nicht erkannt wurde (FRR: False Rejection Rate). Abhängig von der Anwendung muss der Schwellwert gesetzt werden und daraus ergeben sich FAR und FRR. Beispielsweise wird man bei einem Zutrittskontrollsystem zu einem Hochsicherheitstrakt einen unbefugten Zutritt mit hoher Wahrscheinlichkeit verhindern wollen, weshalb der Schwellwert hoch gesetzt wird. Damit sinkt die FAR. Gleichzeitig steigt die FRR, d.h. es wird mehr Fälle geben, in denen eine eigentlich berechtigte Person am Zutritt gehindert wird.

Abhängig vom genutzten biometrischen Charakteristikum kann die Kooperation der betroffenen Person beim Enrolment und beim Abgleich erforderlich sein oder nicht. Während beispielsweise ein Foto problemlos ohne Wissen und Kooperation des Betroffenen erstellt werden kann, muss bei einem Handvenenscanner die Person ihre Handfläche auf den Sensor auflegen. Der Fingerabdruck kann oft sogar noch nachträglich an Orten, an denen sich die betroffene Person aufgehalten hat, abgenommen und gegenüber dem Verfahren präsentiert werden.

2.2.4 Widerstand gegen Verfälschungen

Ein weiterer zu betrachtender Bereich ist das Umgehen des Verfahrens. Das können Verdecker einer Identität sein oder nichtauthentische Personen, d.h. Personen, die gefälschte biometrische Charakteristika präsentieren. Stichwörter sind hier Lebenderkennung und Nicht-Fälschbarkeit. Gerade biometrische Verfahren, bei denen die Kooperation des Betroffenen für das Erfassen des Charakteristikums nicht erforderlich ist, sind anfällig. Ob und inwieweit sich daraus datenschutzrelevante Risiken ergeben, kann nur anhand der gesamten Anwendung beurteilt werden. So kann es erhebliche Auswirkungen auf die Rechte und Freiheiten natürlicher Personen haben, wenn durch die Präsentation gefälschter Charakteristika eine fremde Identität angenommen werden kann.

3 Systeme zur Erfassung biometrischer Charakteristika

Es existiert bereits eine große Anzahl von technischen Systemen, bei denen biometrische Charakteristika ein zentraler Bestandteil der Verarbeitung sind. Biometrische Systeme, deren Zweck die biometrische Erkennung von Individuen durch biometrische Charakteristika ist, lassen sich anhand der folgenden Kriterien systematisieren:

- Welche konkreten biometrischen Charakteristika werden in dem jeweiligen System verwendet (biologische Charakteristika, siehe Kapitel 3.1, und verhaltensabhängige Charakteristika, sowie medizinische Daten als spezielle Untergruppe der biologischen Charakteristika)?
- Mit Hilfe welcher Sensoren, die Teil eines biometrischen Erfassungsgeräts sind, werden die biometrischen Charakteristika erfasst (optische, akustische oder sonstige Sensoren, siehe Kapitel 4)?
- Zu welchem Zweck wird die Verarbeitung der biometrischen Charakteristika durchgeführt?

Es ist davon auszugehen, dass die Anzahl dieser Systeme sowie die Integration der Systeme in komplexe Anwendungen in den nächsten Jahren deutlich an Bedeutung gewinnen werden, da

- die Nutzer bereit sind, diese Systeme zu verwenden (z. B. Nutzung von Wearables zur Aktivitätsmessung, Entsperrung von Smartphones durch Fingerabdruck oder Gesichtserkennung),
- die Integration von Sensoren in digitale Infrastrukturen zunimmt (z. B. Kontaktlinsen, die Blutzuckerwerte messen und übermitteln können) und
- innovative, neue Geschäftsmodelle entwickelt werden, die biologische Eigenschaften verwenden (z. B. Versicherungstarife für „gesunde“ Menschen).

Nicht jedes biometrische Charakteristikum kann allerdings für jeden Zweck verwendet werden.

So werden für die Identifikation oder die Verifikation biometrische Charakteristika benötigt, die „statisch“ sind oder sich nur sehr schwer (z. B. durch plastische Chirurgie) verändern lassen (z. B. Gesicht, Fingerabdruck, Stimme oder das menschliche Genom).

Für Geschäftsmodelle, deren Schwerpunkte vertriebsorientiert sind (Werbung oder Produkte für Personen, die spezielle biologische Eigenschaften aufweisen), werden biologische Eigenschaften verwendet, die „dynamisch“ sind (z. B. Blutdruck, Gewicht), die sich also im Zeitablauf ändern können. Damit können z. B. Zielgruppen definiert und wirtschaftlich erschlossen werden. So ist es möglich, durch ein bestimmtes Verhalten (z. B. Kauf und Verwendung eines Produktes) eine Veränderung dieser biologischen Eigenschaft zu bewirken.

3.1 Erfassung biometrischer Charakteristika

3.1.1 Fingerabdruck/Finger-Bild

Der Fingerabdruck ist ein Abdruck der Papillarleisten am Endglied eines Fingers (Fingerkuppe bzw. Fingerbeere). Da bisher keine zwei Menschen mit dem gleichen Fingerabdruck bekannt sind, geht man von der Einzigartigkeit des Fingerabdrucks aus. Biologisch gesehen ist eine Papillarleiste eine Erhöhung der Epidermis auf der Handfläche oder der Fußsohle. In sehr seltenen Fällen fehlen den Fingern infolge eines genetischen Defekts die Papillarleisten und sie hinterlassen damit keine Abdrücke. Ein vergleichbares Phänomen kann bei Personen auftreten, deren Finger bei der Arbeit oder im Sport stark belastet werden; Beispiele sind Fliesenleger oder Handballer.

Es werden folgende Charakteristika des Fingerabdrucks unterschieden: Grundmuster, grobe Merkmale, feinere Merkmale (Minuzien) und Porenstruktur.

Anhand dieser Charakteristika und ihrer Verteilung innerhalb eines Fingerabdrucks kann eine einzigartige Unterscheidbarkeit gewährleistet werden.

Zur Extrahierung der Minuzien wird ein spezieller Algorithmus verwendet, durch den die Minuzien in eine mathematische Form gebracht werden. Aus dem vom Fingerabdruckscanner gelieferten Bild werden für jeden Fingerabdruck spezifische Daten gesammelt, die zum Einlernen oder späteren Vergleich mit bestehenden Fingerabdruckdaten ausreichen. Ein konkreter Fingerabdruck ist aus den Minuziendaten nicht mehr rekonstruierbar.[5] Es könnte aber ein Fingerabdruck erstellt werden, der ein identisches Template bei einer Prüfung liefert.

3.1.2 Iris

Die Iris ist Teil des menschlichen Auges. Bei der Iris-Erkennung wird über eine Kamera das Farbmuster der Iris erfasst und nach bestimmten Merkmalen (Punkte, Sprenkel, Streifen, Fäden) bewertet.

Zwischen der Iris (Regenbogenhaut) und der Hornhaut des menschlichen Auges liegen komplexe band- und kammartige Bindegewebsstrukturen. Diese Strukturen sind bei jedem Menschen unterschiedlich. Sie unterscheiden sich selbst bei eineiigen Zwillingen. Außerdem verändern sie sich in einem gesunden Auge während eines Lebens wenig. Das mit einer herkömmlichen Kamera (z. B. einer CCD-Kamera[6]) von außen aufgenommen Bild der Iris lässt diese Strukturen erkennen und eignet sich damit als biologisches Charakteristikum.

Bei Menschen mit dunkler Augenfärbung sind die Strukturen im sichtbaren Licht allerdings nur schwer zu erkennen. Biometrische Iriserkennungssysteme beleuchten daher die Iris aus einem Abstand von etwa einem Meter mit für das Auge nahezu unsichtbarem Licht im nahen Infrarotbereich. Dieses durchdringt den "Farbstoff" des menschlichen Auges (Melanin) besser als sichtbares Licht. So kann eine Aufnahme der Irisstrukturen bei allen Menschen mit gesunden Augen angefertigt werden, ohne zu blenden. Aus den aufgenommenen Bildern wird mit speziell für diesen Zweck entwickelten mathematischen Methoden ein eindeutiger Datensatz gebildet, der als Basis für die biometrische Erkennung dient.[7]

3.1.3 Netzhaut (Retina)

Die Retina ist, ebenso wie die Iris, Teil des menschlichen Auges und bezeichnet die Anordnung der Blutgefäße in bzw. hinter der Netzhaut. Die Blutgefäße im Augenhintergrund bilden ein Muster. Durch die Reflexion des eingestrahlten Lichtes an der Retina entsteht ein charakteristisches Gebilde, das von einer Kamera aufgenommen werden kann.[8]

Die Retina ist durch Verteilung, Form und Muster ihrer Blutgefäße individuell eindeutig charakterisiert. Da das exakte Muster der Blutgefäße nicht nur durch genetische Faktoren festgelegt wird, lassen sich selbst eineiige Zwillinge anhand ihrer Retina unterscheiden. Ebenso wie das Irismuster bleibt das Adernmuster der Netzhaut im Verlauf des Lebens weitgehend konstant und macht dadurch die Retina zu einem sehr beständigen Erkennungsmerkmal. Beeinträchtigt werden kann das Muster der Blutgefäße aber durch Krankheiten oder Verletzungen, die dann das Bild der Retina vorübergehend oder andauernd verändern. Zu diesen Krankheiten zählen zum Beispiel Diabetes oder eine Degeneration der Macula, sowie bedingt durch Bluthochdruck geplatzte Kapillargefäße.[9]

Bei der Retina-Erkennung wird der Augenhintergrund einer Person mit Hilfe eines Infrarot-Lichtes sichtbar gemacht. Im Gegensatz zur Iriserkennung, bei der eine herkömmliche Kamera verwendet werden kann, muss bei der Retinaerkennung der Kopf in eine bestimmte Position zum Erfassungsgerät gebracht werden.

---

5 Quelle: https://de.wikipedia.org/wiki/Fingerabdruck

6 CCD: charge coupled device (ladungsgekoppeltes Bauelement), bezeichnet eine Form von Bildsensoren

7 Quelle:https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/BiometrischeVerfahren/Iriserkennung/iriserkennung_node.html

8 Ottenberg, Retinaerkennungssysteme, S. 1, abrufbar unter https://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/07Hand_Retina/retina.pdf

9 Ottenberg, a.a.O., S. 2

3.1.4 Gesicht

Bei der biometrischen Erkennung des Gesichts werden die biologischen Charakteristika der Gesichtszüge anhand eines digitalisierten Bildes, das mit einer Kamera aufgenommen wurde, bestimmt.

Verwendet werden vor allem solche Charakteristika des Gesichts, die sich aufgrund der Mimik nicht ständig verändern, also obere Kanten der Augenhöhlen, die Gebiete um die Wangenknochen und die Seitenpartien des Mundes. Grundsätzlich erfolgt ein Vergleich der Charakteristika mit der entsprechenden biometrischen Referenz mittels klassischer Bildverarbeitungs- und Bildanalyseverfahren, wie etwa nach Lokalisierung der Augen die Berechnung der Gesichtsmerkmale anhand eines Gitternetzes, das über das Gesicht gelegt wird.[10]

3.1.5 Handgeometrie

Jede menschliche Hand ist einzigartig. Ab einem Alter von etwa 20 Jahren sind die Veränderungen an der menschlichen Hand meist nur noch gering. Für die biometrische Erkennung der Handgeometrie wird ein Bild der Hand (im Lesegerät, gespiegelt von einer Kamera), von oben und seitlich aufgenommen.

Aus diesen Bildern werden die Konturen der Hand erzeugt. Daraus werden dann verschiedene biologischen Merkmale extrahiert und ermittelt, z. B. Werte für Dicke, Länge, Breite und Fläche der Hand bzw. der Finger, die Fingerspitzen und Punkte zwischen den Fingern, Handbreite, Abstände und Winkel zwischen verschiedenen Interfinger-Points, Fingerkrümmung und Höhe der Handfläche und Finger.

3.1.6 Venenmuster

Die Venenmuster der menschlichen Hand sind komplex und die Position der Venen ist bei jedem Menschen unterschiedlich und bleibt zeitlebens unverändert, sofern die Hand nicht verletzt wird.

Bei der Erkennung der Venenmuster können entweder die Venen der Handinnenfläche, die Venen des Handrückens oder die Fingervenen mit einem Handvenenerkennungs-Sensor erfasst und zur Identifikation genutzt werden. Dazu sendet der Sensor mittels Infrarot-LEDs Nah-Infrarotstrahlung in Richtung der Handflächen aus. Das sauerstoffreduzierte Blut in den Venen absorbiert diese Infrarotstrahlung mehr als das umgebende Gewebe. Damit kann ein eindeutiges Bild der Venen der Hand/des Fingers aufgenommen und für die Erkennung verwendet werden. Die Venen befinden sich vor Missbrauch und Manipulationen gut geschützt innerhalb des Körpers; für das menschliche Auge sind die Merkmale nicht sichtbar. Hautverunreinigungen oder oberflächliche Verletzungen haben keinen Einfluss.

Handvenenerkennung der Handinnenfläche

Bei diesem Verfahren der Erkennung wird das Venenmuster der Handinnenfläche erfasst und mit späteren Aufnahmen verglichen. Für die Identifikation einer Person muss diese ihre Handinnenfläche flach vor den Sensor des Handvenenscanners platzieren, ohne diesen zu berühren (berührungslose Erfassung). Die Erkennungsrate wird bei dem Verfahren derzeit mit nahezu 100 %, die FAR mit 0,000 08 %, die FRR mit 0,01 % angegeben. Dieses ist somit erheblich genauer als z. B. die Fingerabdruckerkennung.

Einsatzgebiete dieses Verfahrens sind elektronischen Zutrittskontrollen für Bereiche, die die höchste Sicherheit verlangen, wie z. B. Rechenzentren, Kraftwerksbereiche, Sperrzonen auf Flughäfen u. v. m., aber auch als Zugangsschutz bei Rechnern. In einigen Ländern (z. B. Japan) wird das System bereits in Bankautomaten für den sicheren Zahlungsverkehr verwendet.

Die Venenerkennung der Handinnenfläche galt als eines der sichersten Verfahren mit extrem hoher Genauigkeit in der Biometrie bis Dezember 2018, dann wurde öffentlich, dass das System mit entsprechender Technik überlistbar ist. Ein Einsatz unter organisatorisch abgesicherten Bedingungen und mit einer Zwei-Faktor-Authentisierung ist dennoch möglich. Des Weiteren können Lasersysteme für die Blutflusserkennung (Lebenderkennung) zusätzlich als Schutz eingesetzt werden. Bezüglich der

[10] Quelle: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/BiometrischeVerfahren/Gesichtserkennung/gesichtserkennung_node.html

Sicherheit bei Geldautomaten werden weitergehende Überlegungen stattfinden müssen, um von einer gesicherten Anwendung ausgehen zu können.

Handrückenvenenerkennung, Fingervenenerkennung

Bei der Handrückenvenenerkennung wird der Handrücken durch den Sensor eingescannt. Während bei der Handinnenfläche Pigmentflecken oder Haare keine Rolle spielen, kann es beim Handrücken zwangsläufig zu entsprechenden Störungen kommen. Ebenso sind Terminals meist so gebaut, dass ein Griff umfasst werden muss und der Handrücken gegen den Sensor gedrückt wird, wodurch kein berührungsloses Verfahren gegeben ist.

Bei der Fingervenenerkennung wird der Finger von der Oberseite sowie der linken und rechten Seite beleuchtet und das Venenmuster von unten eingescannt. Das Venenmuster eines Fingers ist kleiner und weniger komplex als das Muster der Handfläche. Hinzu kommt die größere Empfindlichkeit der Fingervenen bei Kälte. Bei kalten Fingern können sich die Kapillar-Venen komplett zusammenziehen, so dass sie eventuell nicht mehr erkannt werden. Die Fingervenenerkennung erfolgt nicht kontaktlos, da der entsprechende Finger komplett auf dem Sensor aufliegen muss.

Zusammenfassend kann bezüglich der Handrückenvenenerkennung und Fingervenenerkennung gesagt werden, dass sie aufgrund der Störanfälligkeit vernachlässigbar und kaum im Einsatz sind.

4 Biometrische Sensoren

Ein biometrisches Erkennungssystem setzt sich im Wesentlichen aus den Komponenten Sensor (Messwertaufnehmer), Merkmalsextraktion und Merkmalsvergleich zusammen. Welche Arten von Sensoren zum Einsatz kommen, hängt stark vom biometrischen Charakteristikum ab.

Die Sensorkomponente liefert als Ergebnis ein biometrisches Sample. Die Merkmalsextraktion entfernt mittels Bild- bzw. Datenverarbeitung und -analyse alle vom Sensor gelieferten Informationen, die nicht die geforderten Merkmalseigenschaften erfüllen und liefert als Ergebnis die biometrischen Merkmale. Durch die fest definierte Verkettung der Merkmale entstehen anschließend sogenannte Templates, die keine Rückschlüsse auf die eigentlichen Rohdaten zulassen. Als dauerhafter Speicher kommen in der Regel zentrale Datenbanken zum Einsatz, meist verbleiben im Gerät daher keine weiteren Daten.

Der Merkmalsvergleicher errechnet schließlich einen Vergleichswert (Ähnlichkeitswert; Score) zwischen dem in der Einlernphase erhaltenen oder aus einer externen Datenbank gespeicherten biometrischen Template und dem aktuellen, von der Merkmalsextraktion gelieferten Datensatz. Überschreitet dieser Vergleichswert eine Schwelle, gilt die Erkennung als erfolgreich. Unter Leistungskriterien versteht man, dass die vom biometrischen Sensor gelieferten Samples statistischen Schwankungen unterliegen, die Falscherkennungen bedingen. Die Zuverlässigkeit wird hauptsächlich nach zwei Kriterien beurteilt: nach der Zulassungsrate Unberechtigter (FAR) und nach der Abweisungsrate Berechtigter (FRR).[11] Sämtliche biometrische Verfahren arbeiten nicht fehlerfrei. Sie liefern nur Wahrscheinlichkeitsaussagen über den Grad an Übereinstimmung von aktuell gemessenen und gespeicherten biometrischen Template.

Aufgrund der Komplexität des Themas Biometrie beschränkt sich dieses Positionspapier im Weiteren auf solche Systeme, die biometrische Merkmale erzeugen, indem sie die entsprechenden biometrischen Charakteristika einer betroffenen Person auf Basis optischer Sensoren abbilden. Sollten diese Systeme darüber hinaus üblicherweise auch andere Sensoren wie akustische oder haptische Sensoren beinhalten, so wird für die folgenden Systeme nur die optische Komponente betrachtet.

4.1 Videokameras

Videokameras sind Geräte zur Aufnahme von Bildfolgen in elektrischen Signalen. Im Gegensatz zu Filmkameras lassen sich die gespeicherten Bildsignale direkt sichtbar machen, da nicht erst Filme entwickelt werden müssen. Moderne digitale Videokameras setzen in der Regel auf einen CCD-Chip als Bildaufnehmer. Je größer die Fläche des Bildsensors einer Kamera ist, desto mehr Licht kann sie erfassen. Die Lichtempfindlichkeit steigt und das so genannte Bildrauschen wird verringert.

[11] https://de.wikipedia.org/wiki/Biometrie

Aufgrund der weiten Verbreitung von Videokameras, Smartphones und Webcams, führen die damit ermöglichten biometrischen Auswertungen zu einer schnellen technischen Weiterentwicklung in diesem Bereich: Die Gesichtserkennung ist aktuell eine der besonders weit fortgeschrittenen Formen der biometrischen Analyse. Hierbei wird zwischen Verfahren in 2D und 3D unterschieden, wobei 3D-Verfahren genauere Erkennungen sowie Überwindungssicherheiten leisten sollen, so dass die Gesichtserfassung der Systeme nicht mehr manipulierbar ist.

Bei der biometrischen Gesichtserkennung wird das Gesicht einer Person mit einer Kamera aufgenommen und anschließend mit einem oder mehreren zuvor gespeicherten Gesichtsbildern verglichen. Liefert die Kamera analoge Werte des Gesichtsbildes, werden diese in digitale Formate umgewandelt (digitalisiert). Die Erkennungssoftware lokalisiert das Gesicht und berechnet seine charakteristischen Eigenschaften. Das Ergebnis dieser Berechnungen, das sog. Template, wird mit den Templates der zuvor gespeicherten Gesichtsbilder verglichen.[12]

Der Prozess beim Einsatz von Videokameras zur Gesichtserkennung lässt sich folgendermaßen schematisch darstellen:[13]

- Bilderfassung
- Lokalisierung des Gesichts
- Lokalisierung der Augen und weiterer Gesichtsbereiche
- Normalisierung des Gesichts
- Merkmalsextraktion
- Templateerstellung

Das Bild des Gesichts einer Person wird mittels einer Kamera im aktuellen Umfeld aufgenommen oder in Form eines Scans eines bereits vorhandenen Bildes der Person erfasst. Der nächste Schritt besteht aus einer Gesichtsdetektion, die die Bildinformationen auf gesichtsähnliche Formen untersucht. Sofern ein Gesicht lokalisiert wurde, werden typischerweise im nächsten Schritt die Augen detektiert, da sie sich in der Regel aufgrund anderer Färbung vom restlichen Gesicht abheben. Abhängig vom eingesetzten Algorithmus werden weitere Gesichtsbereiche lokalisiert und anschließend das Gesicht normalisiert, um die Daten invariant gegenüber Drehung, Streckung und Stauchung zu speichern. Auf Basis dieser normalisierten Gesichter erfolgt dann die Merkmalsextraktion, die ebenfalls vom verwendeten Verfahren abhängig ist. Aus den Merkmalen werden im letzten Schritt mittels mathematischer Formulierungen Merkmalsvektoren generiert.

4.2 Infrarotkameras

Im Gegensatz zu Videokameras erfassen Infrarotkameras nicht das für das menschliche Auge sichtbare Licht, sondern elektromagnetische Strahlung im Infrarot-Bereich.

Nutzung zur Wärmebilderfassung

Bei der Wärmebilderfassung wird über die Intensität der Strahlung im Infrarotbereich auf die Temperatur eines Objekts geschlossen. Der Zusammenhang zwischen Strahlung und Temperatur wird mittels Boltzmann-Konstante hergestellt (Intensität der Strahlung = Boltzmann-Konstante * Temperatur) Das elektromagnetische Spektrum liegt bei Infrarotstrahlung zwischen 0.8 und 14 µm Wellenlänge, fällt also nicht in den für das menschliche Auge sichtbaren Bereich von 0.4 bis 0.7 µm.

Nutzung als Tiefenkameras (bspw.: Apple FaceID, Microsoft Kinect)

Tiefenkameras wurden ursprünglich zur Bewegungserkennung als natürliche Interaktion zwischen Mensch und Computer eingeführt.[14] Ein IR-Projektor sendet im nahen Infrarotbereich ein für das menschliche Auge nicht sichtbares codiertes Punktmuster aus. Ein CMOS-Sensor[15] empfängt das von der Szene reflektierte Bild und berechnet, aufgrund des Kameraabstandes über die Parallaxen korrespondierender Punkte, ein Tiefenbild. Punkte gleicher Größe wirken bei unterschiedlicher

[12] BSI, Gesichtserkennung, S. 1, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf
[13] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf
[14] http://www.scanner.imagefact.de/de/depthcam.html
[15] CMOS: complementary metal oxide semiconductor („komplementärer Metalloxid-Halbleiter“): eine bestimmte Form von Halbleiterbauelementen

Entfernung unterschiedlich groß, bei bekannter Punktgröße kann auf die Entfernung zurückgeschlossen werden.

Nutzung zur Venenerkennung

Die Venenerkennung ist ein biometrisches Verfahren, mit dem Personen durch Infrarot-Technologie anhand ihrer Handgefäßstruktur erkannt werden können. Der Verlauf der Adern und Venen ist dabei genauso einzigartig wie der Fingerabdruck. Sensoren, die auf die Temperatur der Gefäßstruktur in der Hand reagieren, stellen in Kombination mit komplexer Filtertechnologie eine sogenannte Lebenderkennung fest und sollen somit vor Täuschungsversuchen mittels nichtbiometrischer Mittel oder durch Nachbildung biometrischer Merkmale schützen.

4.3 Fingerabdruckleser

Der Prozess einer Fingerabdruckanalyse lässt sich in folgenden Schritten schematisch darstellen:[16]

- Aufnahme des Fingerabdruckbildes
- Bildqualitätsverbesserung
- Bildaufarbeitung
- Musterklassifizierung
- Merkmalsextraktion
- Verifikationsphase

Der grundlegende Aufbau eines optischen Fingerabdrucklesers besteht aus einer Lichtquelle, einem Glasprisma, einer Linse und einem Bildsensor. Der Finger wird auf das Glasprisma gedrückt, dabei haben Erhebungen direkten Kontakt mit dem Prisma, nur zwischen den Tälern und dem Prisma ist noch Luft. Das Licht wird von einer Seite ins Prisma gesendet. Es wird dann an den Tälern reflektiert und an den Erhebungen absorbiert bzw. zufällig gestreut. Die reflektierten Strahlen, die das Prisma verlassen, werden außerhalb durch die Linse auf einen Bildsensor gebündelt, in dem die Aufnahme stattfindet.

Bei jedem Sensor entsteht als Endprodukt im Allgemeinen ein Graustufenbild des Fingerabdruckes. Um ein Graustufenbild zu generieren gibt es zwei Modi: Beim *live scan* wird der Fingerabdruck durch einen Sensor aufgenommen, beim offline-Modus wird eine Aufnahme von hinterlassenen Fingerabdrücken, z. B. Gläsern, gemacht. Die Rohdaten werden mittels Bildverarbeitung verbessert und aufbereitet. Anschließend wird die Lage der Minuzien (Gabelung und Linienendung) in dem Fingerabdruck detektiert und extrahiert. In der Praxis weisen die aufgenommenen Fingerabdruckbilder eine unterschiedliche Qualität auf. Die Leistungsfähigkeit der Algorithmen kann durch mangelnde Bildqualität, verursacht durch Schmutz oder Verletzungen, beeinträchtigt werden.

Schließlich werden Entscheidungen, ob der ermittelte Merkmalsvektor einer vorhandenen Entität entspricht, auf Basis von Vergleichen zweier Merkmalsvektoren durchgeführt.

4.4 Handgeometrieleser

Bei der Handerkennung sind relevante biometrische Merkmale die Höhe und Breite des Handrückens und der Finger, sowie deren relative Lagen. Nicht relevant sind der Abdruck der Handflächen und die Fingerspitzen, da die Nägel nachwachsen und geschnitten werden.[17] Die Komponenten eines Handgeometrielesers sind meist in einem Gerät integriert. Dazu gehören eine CCD-Kamera zum Erfassen der Merkmale in Form einer 3D-Bildaufnahme, ein Display zur Interaktion mit dem Nutzer (Anzeige fehlerbehafteter Bereiche), ein Prozessor zum Erstellen und Überprüfen der Templates und ggf. Lesegeräte für ID-Karten oder PIN-Eingaben. Softwareseitige Komponenten sind vom jeweiligen Anwendungsfall abhängig.

Die Handerkennung erfordert eine korrekte Positionierung der Hand. Diese wird durch Orientierungshilfen erleichtert und durch visuelle Rückmeldung auf dem Display verdeutlicht.

---

[16] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/BiometrischeVerfahren/Fingerabdruckerkennung/fingerabdruckerkennung_node.html

[17] https://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/07Hand_Retina/Handerkennung-Ausarbeitung.pdf

Die Merkmalserfassung erfolgt durch eine CCD-Kamera, die mindestens zwei 3D-Bilder erstellt, je eines von oben und von der Seite. Definierte Charakteristika werden erfasst und in die Merkmale in Templates mit einer Größe von wenigen Byte gespeichert. Typischerweise werden nur um die 100 Charakteristika erfasst, was direkt eine geringe Einzigartigkeit zur Folge hat. Daher eignet sich dieses Verfahren weniger gut für die eindeutige Erkennung einer Person als z. B. Venenerkennung. Es kann allerdings zum Beispiel durch den Einsatz robuster Algorithmen „optimiert“ werden.[18]

4.5 Irisscanner

Der Prozess bei Irisscannern lässt sich schematisch folgendermaßen darstellen:[19]

- Bildaufnahme der Iris (Regenbogenhaut des Auges), meist im Nah-Infrarot-Bereich
- Iriserkennung
- Irissegmentierung
- Transformation des Kreissegments auf einen Streifen
- Binarisierung und Templateerstellung

Im Irisscanner wird die Iris durch eine Kamera erfasst und durch Bildverarbeitung isoliert, indem zwei Kreise (außen und innen) als Begrenzung der Iris dienen. Der resultierende Ring wird durch Polarkoordinaten repräsentiert, wodurch Invarianzen zur Irisgröße/-dicke ermöglicht werden. Daraufhin erfolgt eine spiralförmige Abtastung der Aufnahme und eine Gruppierung in helle und dunkle Bereiche (Binarisierung). Durch „Ausrollen“ der Spirale kann eine Grafik, ähnlich eines Barcodes, generiert werden, die entsprechend mit den Templates verglichen wird.

Kommerzielle Erkennungsverfahren erfassen etwa 260 individuelle optische Merkmale der Iris. Diese Merkmale entwickeln sich aus einem zufallsgesteuerten, morphogenetischen Prozess in den ersten Lebensmonaten einer Person und bleiben über die restliche Lebenszeit weitgehend unverändert. Auch eineiige Zwillinge haben keine identische Iris-Struktur.[20]

4.6 Retinascanner

Der Prozess bei Retinascannern lässt sich folgendermaßen darstellen:

- Bildaufnahme der Retina (Netzhaut des Auges) durch kreisrunde Abtastung mit einem Laser
- Bildkorrektur bei Fehlsichtigkeiten der Linse
- Korrektur von Verdrehungen des Kopfes/der Retina
- Binarisierung und Templateerstellung

Der Retinascanner tastet die Retina mit einem Infrarot-Laser kreisrund ab. Eventuell vorhandene Fehlsichtigkeiten der Personen können und müssen bis zu gewissen Ausprägungen korrigiert werden, da ansonsten keine Normierung innerhalb der Template-Datenbank gegeben wäre. Das Phasen-Korrektur-Modul sorgt für die Bildkorrektur, falls der Kopf bzw. die Retina bei der Aufnahme verdreht erfasst wurde. Hierzu muss das digitale Abbild mehrfach in kleinen Schritten zum Referenzobjekt in der Datenbank verschoben und die Korrelation zwischen den jeweiligen Verschiebungen und der Referenz gebildet werden. Dadurch, dass Adern auf der Retina den Laserstrahl stärker absorbieren als umliegendes Gewebe, setzen sie sich kontrastreicher ab. Für die Binarisierung und Templateerstellung werden Schwellwerte definiert, sodass sich die Bildinformationen der Blutbahnen von den restlichen Strukturen trennen lassen.

Je nach Hersteller erfolgt der Scan-Vorgang auf unterschiedlich definierte Weise, sodass es nicht direkt möglich ist, Systeme unterschiedlicher Hersteller miteinander zu vergleichen. Weiterhin unterliegt die Retina degenerativen Veränderungen, sodass es im Laufe des Lebens zu unterschiedlichen Templates kommen kann. Die Retina eineiiger Zwillinge unterscheidet sich ebenfalls.

---

[18] Singh, Hand geometry verification system: A review, S. 4, https://www.researchgate.net/profile/Amit_Singh202/publication/224086092_Hand_geometry_verification_system_A_review/links/5681052908ae1975838ead2f/Hand-geometry-verification-system-A-review.pdf?origin=publication_detail

[19] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Iriserkennung_pdf.pdf

[20] https://de.wikipedia.org/wiki/Iris-Erkennung#Eigenschaften

5 Sammlung möglicher Einsatzszenarien („Use Cases“)

5.1 Übersicht über Einsatzszenarien

Es gibt zahlreiche Szenarien, bei denen biometrische Verfahren zum Einsatz kommen. Dies sind einerseits Szenarien, bei denen biometrische Erkennungssysteme mit dem unmittelbaren Ziel einer Identifikation oder Verifikation von Personen betrieben werden. Daneben gibt es Szenarien, bei denen Daten aus Verwendungszusammenhängen (etwa Videoüberwachung, Audiomitschnitte) mit Hilfe biometrischer Verfahren ausgewertet werden. Bei einigen dieser Verfahren ist ebenfalls eine Identifikation von Personen das Ziel; andere Verfahren zielen auf eine Wiedererkennung von Personen oder eine Gruppenzuordnung (Gefühlserkennung, Altersschätzung) ab. Szenarien sind u. a.:

- Identifikation
- Verifikation
- Wiedererkennung
- Profilbildung
- Gefühlsanalyse
- Beobachtung/Überwachung
- Registrierung
- Verhaltenssteuerung
- Werbung / Marketing
- Kommunikation
- Interaktion (Mensch – Maschine)

Die Einsatzszenarien aus Abschnitt 5.1 lassen sich unter verschiedenen Blickwinkeln gruppieren. Dazu gehören zum einen technische und funktionale Aspekte der biometrischen Verfahren, zum anderen die Zwecke, die mit dem Einsatz verfolgt werden.

5.2 Klassifikation der Szenarien nach technischen und funktionalen Aspekten

5.2.1 Kooperative biometrische Verifikation

Eine typische Funktion biometrischer Verfahren sind Authentisierungsverfahren (z. B. Zutrittskontrolle, Login, Entsperren), die kooperativ erfolgen: Die zu authentisierende Person verwendet das biometrische Verfahren bewusst mit dem Ziel, vom System erkannt zu werden (bewusste und kooperative Präsentation). Auch automatisierte Passkontrollen, bei denen die Übereinstimmung der in Ausweispapieren gespeicherten biometrischen Daten mit aktuell gewonnen Daten des Reisenden verglichen werden, fallen in diese Kategorie.[21] Gegebenenfalls sind mehrere Versuche bis zu einer positiven Authentisierung erforderlich. Zum Einsatz kommen Identifikations- und Verifikationsverfahren.

5.2.2 Nicht-kooperative biometrische Erkennung

Weitere typische Anwendungsfälle sind Überwachungsszenarien, bei denen eine Identitätsfeststellung (Identifizierung) oder Überprüfung einer Identität in einer Weise erfolgt, bei der die Person nicht kooperieren muss. Dies ist der Fall, wenn die biometrischen Charakteristika ohne bewusste Handlungen (kooperative Präsentation) der Person erfasst werden (können). Beispiele sind Video- oder Audioaufnahmen, die offen oder verdeckt erstellt werden oder die Auswertung anderweitig erfasster Daten (etwa Videoaufnahmen, Telefonate, Tastaturnutzungen) mit dem Ziel einer biometrischen Verarbeitung. Dies kann im Modus der bewussten oder indifferenten Präsentation erfolgten. Typische Szenarien sind hier Fahndungen oder Vergleiche mit biometrischen Referenz-Datenbanken im Sinne einer Identifikation.

In die Kategorie nicht-kooperativer Verfahren würde auch eine zwangsweise Nutzung biometrischer Verfahren aus dem Abschnitt 5.2.1 fallen.

[21] Im Zusammenhang mit Grenzkontrollen sind weitere Nutzungen der aktuell gewonnen biometrischen Daten der Reisenden denkbar, etwa der Abgleich mit biometrischen Datenbanken (z. B. Fahndungsdatenbanken) im Hintergrund. Eine solche Nutzung ist dem Szenario 5.2.2 Nicht-kooperative biometrische Erkennung zuzuordnen.

5.2.3 Zuordnung zu Gruppen

Biometrische Verfahren werden nicht nur mit dem Ziel betrieben, einen eindeutigen Personenbezug herzustellen. Anwendungen können auch eine automatisierte Schätzung demographischer Daten (z. B. Alter, Geschlecht) oder die Zuordnung zu einer Gruppe (z. B. Altersgruppe, Brillenträger, Haar- und Augenfarbe, Zuordnung zu einer Ethnie etc.) vornehmen. Diese nicht personenindividuellen Merkmale werden auch als „soft biometrics“ bezeichnet. Hierbei kommen in erster Linie Abbildungen von Gesichtern und der Iris zum Einsatz; denkbar sind auch Sprach- und Dialekterkennungen.

Die Zuordnung zu Gruppen mit Hilfe von „soft biometrics“ kann auch verwendet werden, um die Anzahl der zu vergleichenden biometrischen Daten in Identifikationsverfahren zu reduzieren, wenn die zum Vergleich verwendeten biometrischen Daten ebenfalls klassifiziert sind (Beispiel: Geschlechtserkennung der aktuellen Person und Suche in Datenbanken nur bei Personen gleichen Geschlechts).

5.2.4 Profilbildung, Verkettung

Weiterhin können biometrische Verfahren mit dem Ziel betrieben werden, Handlungen einzelner Personen zu verketten. Ein typisches Beispiel ist die „Verfolgung“ von Personen bei einer Videobeobachtung: Technisch liegen Videoaufzeichnungen als Datenstrom vor, der aus einzelnen Bildern (Frames) besteht. Die schnelle Abfolge beim Abspielen ergibt den Eindruck eines Films (wie beim Daumenkino). Sollen Personen gezählt oder eine Verweildauer ermittelt werden, so muss über mehrere Frames hinweg verglichen werden, ob es sich um dieselbe Person handelt oder nicht. Eine Identifizierung der Person ist nicht erforderlich.

5.2.5 Verhaltenserkennung

Verfahren können auch mit dem Ziel betrieben werden, Verhaltensweisen zu erkennen und die betroffenen Personen einer Verhaltensgruppe zuzuordnen. Beispielsweise lässt sich aus Gesichtsaufnahmen auf Gefühle (erregt, freundlich, ablehnend etc.)[22] schließen; ebenso aus Tonaufnahmen.

5.3 Betrachtung der Szenarien nach Zwecken im datenschutzrechtlichen Sinn

5.3.1 Hoheitliche Authentisierungsverfahren

Typische Beispiele hoheitlicher Authentisierungsverfahren sind automatisierte Überprüfungen von biometrischen Daten (Gesichtsbild, Fingerabdruck) aus hoheitlichen Dokumenten (Reisepässe, Personalausweis, Aufenthaltstitel) mit den biometrischen Charakteristika des Ausweisinhabers.

5.3.2 Staatliche Identifikationsverfahren

Identifikationsverfahren kommen zum Einsatz, um einerseits unbekannte Personen erstmalig zu identifizieren (Identitätsfeststellung) oder um Doppelidentitäten zu entdecken. Ein Beispiel für den ersten Fall sind Abgleiche von Täterfotos (etwa auch Überwachungskameras von Geldautomaten) oder Videoaufzeichnungen mit Datenbanken, bei denen die biometrischen Daten mit identifizierenden Metadaten (z. B. einem Namen) verknüpft sind. Ein Beispiel für den zweiten Fall ist der Einsatz von Erkennungssystemen zur Aufdeckung von Doppelidentitäten, etwa bei Asylbewerbern.

5.3.3 Zutrittskontrolle

Das biometrische Verfahren wird zur Kontrolle eines physischen Zutritts zu Räumen oder Gebäuden verwendet. Typische verwendete biometrische Charakteristika sind Gesichtsform und Fingerabdrücke; andere Charakteristika wie Handgeometrie und Iris kommen auch zum Einsatz.

5.3.4 Zugangskontrolle

Das biometrische Verfahren wird zur Kontrolle des Zugangs zu Datenverarbeitungssystemen verwendet. Typische Szenarien sind die Entsperrung von Mobilgeräten mit Hilfe der biometrischen

[22] Siehe z. B. die „Emotion-API“ der Firma Microsoft, https://azure.microsoft.com/de-de/services/cognitive-services/emotion/?cdn=disable oder https://www.heise.de/newsticker/meldung/Software-erkennt-Gefuehle-2123851.html

Charakteristika Gesichtsform und Fingerabdruck, aber auch Authentisierungsmechanismen (Log-in) auf Betriebssystemebene mit Hilfe von Gesichtsform und Fingerabdruck.

5.3.5 Werbung, Marketing

Werbe- und Marketingmaßnahmen können mit Hilfe biometrischer Verfahren auf bestimmte Gruppen, einzelne Personen oder auch deren Verhaltensweisen zugeschnitten werden.

Im ersten und dritten Fall werden die Zielpersonen Gruppen zugeordnet (z. B. Alter, Geschlecht, Bartträger, Brillenträger im ersten Fall, Gruppe der Ärgerlichen, Freundlichen oder Neutralen im dritten Fall) und entsprechende gruppenspezifische Werbemaßnahmen ausgewählt. Eine Identifizierung ist nicht erforderlich und wird auch meist nicht angestrebt; die Zuordnung zu einer Gruppe ist ausreichend. Wie bei der biometrischen Erkennung kann die Zuordnung zu einer Gruppe fehlerbehaftet sein.

Je nach Konstellation kann die Zuordnung zu einer Gruppe unter die Kategorie besonderer Daten fallen, wenn beispielsweise Gruppen nach sexuellen Präferenzen[23], Hautfarben oder körperlichen Einschränkungen gebildet werden.

Im zweiten Fall (Werbemaßnahmen für einzelne Personen) ist eine biometrische Erkennung erforderlich. Diese kann sich auf namentlich bekannte Personen (etwa VIPs, Stammkunden) und somit auf Personen mit bekannten Metadaten beziehen. Denkbar sind aber auch Fälle, bei denen lediglich eine Wiedererkennung („besucht zum dritten Mal in dieser Woche den Supermarkt“) erfolgt, ohne dass Metadaten zu einer Identifizierung verwendet werden.

5.3.6 Reichweitenmessung von Werbung

In einem weiteren Szenario wird mittels biometrischer Verfahren detektiert, durch welche Gruppen und wie lange Werbung betrachtet wird. Dazu werden während einer Werbemaßnahme die Betrachter erfasst und einer Gruppe zugeordnet (etwa Geschlecht oder Alter, siehe Abschnitt 5.3.5 Werbung, Marketing, 1. Fall) und die Betrachtungsdauer gemessen. Ebenso wird versucht, Reaktionen auf Werbemaßnahmen (Gefühlsregungen) zu erfassen. Hierbei kommen in erster Linie Verfahren zum Einsatz, die die biometrische Charakteristika des Gesichts auswerten.

5.3.7 Beobachtung, Überwachung

In einem Überwachungsszenario werden biometrische Charakteristika (in erster Linie Gesichtsbilder und Sprache) erhoben (Video- und Audioaufnahmen) und mit bekannten biometrischen Daten, etwa aus einer Sperrliste (z. B. Personen mit Hausverbot) verglichen („Watchlist“). Dies kann mit hoheitlichen Anwendungen verknüpft werden (siehe Abschnitt 5.3.2).

5.3.8 Mensch-Maschine-Interaktion, Steuerung

Bei Interaktionen und Steuerungen von Maschinen können ebenfalls biometrische Verfahren zum Einsatz kommen. Beispiele reichen hier von einer reinen Anwesenheitserkennung über die Detektion von Aufmerksamkeit und Position von Personen in Kraftfahrzeugen (teilautonomes Fahren), einer Einschätzung aktueller Verhaltensweisen (defensive/sportliche Fahrweise) bis zu einer Personenerkennung des Fahrers mit dem Ziel einer individuellen Konfiguration des Fahrzeugs (Sitz- und Spiegelposition, Radiosender).

In einen ähnlichen Anwendungsbereich fällt eine Gruppenzuordnung von Personen aus dem Umfeld des Kfz (etwa zur Unterscheidung von Altersgruppen von Passanten mit dem Ziel, beim Erkennen von Kindern bremsbereit zu sein).

Andere Steuerungsmechanismen basieren auf einer Sprechererkennung, etwa im Bereich der Heimautomatisierung.

Nicht alle dieser Anwendungen erfordern die Identifikation von Personen. So kann mit biometrischen Verfahren ermittelt werden, ob Fahrerinnen und Fahrer hinreichend konzentriert sind.

[23] Siehe z. B. http://www.spiegel.de/netzwelt/netzpolitik/software-kann-homosexuelle-anhand-von-fotos-erkennen-a-1166971.html

6 Rechtliche Bewertung

Nach Art. 9 Abs. 1 DS-GVO ist die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person grundsätzlich untersagt. In den in Art. 9 Abs. 2 DS-GVO normierten Fällen ist sie ausnahmsweise erlaubt. Erfolgt die Verarbeitung biometrischer Daten nicht zur eindeutigen Identifizierung einer natürlichen Person, sondern zu einem anderen Zweck, richtet sich ihre Zulässigkeit nach Art. 6 Abs. 1 DS-GVO. In jedem Fall ist die Eignung biometrischer Daten zur eindeutigen Identifizierung im Wege biometrischer Analyseverfahren bei der Risikoabschätzung und der Auswahl der technischen und organisatorischen Maßnahmen zu berücksichtigen.

6.1 Begriff der biometrischen Daten nach Art. 4 Nr. 14 DS-GVO

Biometrische Daten sind nach der Definition in Art. 4 Nr. 14 DS-GVO mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

6.1.1 Personenbezogene Daten

Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Im Prinzip ist jedes eindeutige biometrische Merkmal ein individuelles Personenkennzeichen[24] und daher ein personenbezogenes Datum.

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten nach Erwägungsgrund 26 alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Durch den ausdrücklichen Bezug auf die technologische Entwicklung dynamisiert die DS-GVO den Begriff der Identifizierbarkeit und verpflichtet Verantwortliche, Aufsichtsbehörden und Gerichte, in Zukunft dieser Entwicklung zu folgen und gegebenenfalls die Identifizierbarkeit von Datenbeständen neu zu bewerten. Um den Zweck des Schutzes der betroffenen Personen vor Beeinträchtigung ihrer Grundrechte durch die Verarbeitung von Daten zu erreichen, müssen die tatsächlich verfügbaren und nicht nur die rechtlich zulässigen Möglichkeiten berücksichtigt werden.[25]

Die Grundsätze des Datenschutzes sollten nach Erwägungsgrund 26 nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Nichts am Personenbezug der verarbeiteten Daten ändert hingegen deren Pseudonymisierung. Gemäß Art. 4 Nr. 5 DS-GVO ist Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Da der Verantwortliche weiterhin in der Lage ist, die betroffenen Personen zu identifizieren, bleibt der Personenbezug pseudonymisierter Daten erhalten. Das ergibt sich auch aus Erwägungsgrund 26.

[24] Weichert, Biometrie - Freund oder Feind des Datenschutzes? in: CR 1997, S. 369.
[25] Klabunde, in: Ehmann/Selmayr, DS-GVO, Art. 4 Rn. 13

Nach Ansicht der früheren Artikel-29-Datenschutzgruppe[26] gilt ein Referenz-Template, das von dem Bild einer Person geschaffen wurde, als personenbezogenes Datum, da es einen Satz unverwechselbarer Merkmale des Gesichts einer Person enthält, der dann mit einer bestimmten Person verlinkt wird und als Referenz für spätere Vergleiche zur Identifizierung und Verifizierung gespeichert wird.

6.1.2 Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person

Mit biometrischen Daten im Sinne der DS-GVO werden Seins-Merkmale wie körperliche Eigenschaften oder Verhaltensweisen angesprochen, die unmittelbar einer Person zugeordnet werden können und in der Regel dauerhaft an eine Person gebunden sind. Eine (beabsichtigte oder unfreiwillige) Trennung von der Person kann grundsätzlich nicht stattfinden.[27] Die biologischen oder verhaltensabhängigen Charakteristika eines Individuums, von welchem sich zur Unterscheidung verwendbare, reproduzierbare biometrische Merkmale ableiten lassen, die zum Zweck der automatisierten biometrischen Erkennung einsetzbar sind, nennt man „biometrische Charakteristika“. Sie sind der Ausgangspunkt für alle biometrischen Erkennungssysteme.

6.1.3 Daten, die die eindeutige Identifizierung einer natürlichen Person ermöglichen oder bestätigen

Biometrische Daten sind zur eindeutigen Identifizierung einer natürlichen Person geeignet, wenn die gemessenen Merkmale einzigartig sind. Nicht notwendig ist, dass die Angaben weltweit eindeutig sind. Es genügt, dass eine genaue Identifizierung in einer mit abstrakten Merkmalen beschriebenen Gruppe einer großen unbestimmten Zahl von Personen möglich ist. Relevant ist, dass die über die natürliche Person erfassten Daten objektiv unverwechselbar sind. Wegen ihrer Verbindung mit dem menschlichen Körper sind sie nicht oder nur schwer zu verändern oder zu verfälschen. Dessen ungeachtet können sich z. B. auf Grund des Alters oder von Krankheiten Veränderungen ergeben, die eine Zuordnung erschweren oder gar unmöglich machen. Auch das Fehlen von bestimmten biometrischen Merkmalen (etwa von Fingerabdrücken) bei einer bestimmten Person kann zu deren Identifizierung geeignet sein.[28]

6.1.4 Mit speziellen technischen Verfahren gewonnene Daten

Die Definition nimmt Bezug auf „spezielle technische Verfahren“. In der englischen Fassung wird hier der Begriff „specific technical processing“ benutzt, also „bestimmte technische Verfahren“.[29] Dabei kann es sich nur um solche Verfahren handeln, die Daten liefern, die nach dem Stand der Technik die eindeutige Identifizierung einer natürlichen Person mit einem biometrischen Erkennungssystem ermöglichen.

Hierzu ist es erforderlich, dass der Informationsgehalt der Daten für eine eindeutige Identifizierung ausreicht. Biometrische Daten sind daher sowohl die biometrischen Samples, also die direkt mit einem Sensor erfassten Merkmale, wie auch die so genannten Templates, das heißt die aus biometrischen Samples gewonnenen und typisierten Merkmals-Vektoren, die auf der Grundlage eines mathematischen Modells standardisiert erfasst und regelmäßig zur Grundlage für digitale Zuordnungen genommen werden[30].

6.1.5 Verhältnis zum Begriff der biometrischen Daten nach ISO/IEC JTC SC37

Nach dem durch das nach ISO/IEC JTC SC37 international standardisierten biometrischen Vokabular sind biometrische Daten biometrische Samples oder Ansammlungen biometrischer Samples in jeder Verarbeitungsstufe, biometrische Referenzen, biometrische Proben, biometrische Merkmale oder biometrische Eigenschaften. Demgegenüber sind biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die

---

[26] Die Artikel-29-Datenschutzgruppe war ein unabhängiges Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes. Mit dem Inkrafttreten der Datenschutzgrundverordnung wurde die Artikel-29-Datenschutzgruppe durch den Europäischen Datenschutzausschuss (EDSA) abgelöst. Der EDSA hat sich dazu noch nicht geäußert.

[27] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/AllgemeineEinfuehrung/einfuehrung.html

[28] Weichert, in Kühling/Buchner, DS-GVO, Art. 4 Nr. 14, Rn. 2.

[29] Im Folgenden wird daher dieses Begriffsverständnis zugrunde gelegt.

[30] Weichert, a.a.O., Rn. 7.

eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen. Sowohl die DS-GVO als auch das international standardisierte Vokabular haben jedoch die Verarbeitung biometrischer Verfahren zum Zweck der eindeutigen Identifizierung im Fokus.

Der Begriff der biometrischen Daten aus dem international standardisierten biometrischen Vokabular kann daher zur näheren Bestimmung des Begriffs der biometrischen Daten nach Art. 4 Nr. 14 DS-GVO herangezogen werden. Allerdings zählen nach dem biometrischen Standard-Vokabular auch solche biometrischen Eigenschaften zu den biometrischen Daten, die nicht für sich genommen die eindeutige Identifikation einer natürlichen Person ermöglichen. Daten wie Alter, Größe und Geschlecht, bei denen es sich zwar um biometrische Daten im Sinne des biometrischen Standardvokabulars handelt, dürften grundsätzlich nicht allein die eindeutige Identifizierung einer natürlichen Person im Sinne der DS-GVO ermöglichen. Je nach Einzelfall kann es hiervon Ausnahmen geben. So genügt zur eindeutigen Identifizierung einer natürlichen Person die Angabe des Geschlechts, wenn es in einer Gruppe von Menschen nur eine Person dieses Geschlechts gibt.

Als biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO können danach sowohl die biometrischen Samples, also die analogen oder digitalen Repräsentationen biometrischer Charakteristika vor der biometrischen Merkmalsextraktion, als auch die biometrischen Merkmale, das heißt die Zahlen oder markanten Kennzeichen, die aus einem biometrischen Sample extrahiert wurden und zum Vergleich verwendet werden können, eingestuft werden.

Klarere Konturen erhält der Begriff der biometrischen Daten ferner dadurch, dass das international standardisierte biometrische Vokabular die biometrische Erkennung als automatisierte Erkennung beschreibt, also als die Erkennung mittels eines rechnergestützten Systems. Das bedeutet, dass von biometrischen Daten erst dann die Rede sein kann, wenn diese für eine automatisierte Verarbeitung geeignet sind. Dieses Begriffsverständnis passt zu dem der DS-GVO: Danach sind biometrische Daten mit speziellen technischen Verfahren gewonnene Daten. Dies setzt ein zumindest teilweise automatisiertes Verfahren zur Gewinnung voraus. Zudem ist eine automatisierte Verarbeitung biometrischer Daten mittels biometrischer Erkennungsverfahren zum Zwecke der eindeutigen Identifizierung für die betroffenen Personen mit erhöhten Risiken verbunden. Die so verarbeiteten Daten sind deshalb nach Art. 9 Abs. 1 DS-GVO als besondere Kategorie personenbezogener Daten einzustufen, deren Verarbeitung nach Art. 9 Abs. 2 DS-GVO einer besonderen Rechtfertigung bedarf.

6.1.6 Beispiele für biometrische Daten gemäß Art. 4 Nr. 14 DS-GVO

6.1.6.1 Fingerabdrücke

Eine Aufnahme der Papillarleisten an der Fingerkuppe ist ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen einer Person. Sie lässt sich einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einer solchen Aufnahme handelt es sich um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.2 Aufnahmen der Irisstrukturen

Eine Aufnahme der Irisstrukturen ist ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen einer Person. Sie lässt sich einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einer solchen Aufnahme handelt es sich um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.3 Retinascans

Ein Retinascan ist ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen einer Person. Er lässt sich einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einem Retinascan handelt es sich um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.4 Handvenenbilder

Ein Bild des Handvenenmusters ist ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen einer Person. Es lässt sich einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einem Bild des Handvenenmusters handelt es sich um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.5 Handgeometrie

Aufnahmen der Handgeometrie sind mit einem speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physiologischen Merkmalen einer Person. Sie lassen sich einer natürlichen Person eindeutig zuordnen und ermöglichen dadurch die eindeutige Identifizierung einer natürlichen Person. Bei den Aufnahmen handelt es sich um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.6 Gesichtsbilder

Ein Gesichtsbild ist dann ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen einer Person, wenn dieses die Verarbeitung biometrischer Charakteristika des Gesichts zur Erstellung eines biometrischen Templates oder strukturierter Sammlungen von Gesichtsbildern ermöglicht. Das Gesichtsbild lässt sich dann im Rahmen eines automatisierten Verfahrens einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einem Gesichtsbild handelt es sich unter den vorgenannten Voraussetzungen um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

Im Gegensatz zu Gesichtsbildern (wie in Art. 4 Nr. 14 DS-GVO als biometrisches Datum genannt) sind Lichtbilder oder Videoaufnahmen von Personen nicht per se biometrische Daten gem. Art. 4 Nr. 14 DS-GVO.

Auf Lichtbildern oder Videoaufnahmen können aber biometrische Daten enthalten sein, wenn das Gesicht einer Person in entsprechender Auflösung, Ausrichtung und Größe auf dem Lichtbild oder der Videoaufnahme abgebildet wird.

6.2 Voraussetzungen des Art. 9 DS-GVO

6.2.1 Grundsätze

Die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ist gemäß Art. 9 Abs. 1 DS-GVO grundsätzlich untersagt. Eine Verarbeitung im Sinne des Art. 9 Abs. 1 DS-GVO liegt vor, wenn die eindeutige Identifizierung einer natürlichen Person im Vordergrund steht. Die englische Fassung wird noch deutlicher, da hier von „the purpose of uniquely identifying a natural person“ die Rede ist. Dies macht klarer als das deutsche „um … zu“, dass hier der Zweck (purpose) einer eindeutigen Identifizierung hinter der Verarbeitung stehen muss.

Identifizierung im Sinne der Verordnung umfasst nicht jedwede Erkennungsmöglichkeit im Zusammenhang mit biometrischen Daten. Zielrichtung des Art. 9 DS-GVO ist es, die Verarbeitung von besonders sensiblen personenbezogenen Daten einzuschränken und nur unter besonderen Voraussetzungen zuzulassen. Biometrische Daten zählen aufgrund ihrer Vielfältigkeit nur dann zu diesen Daten, im Gegensatz zu den übrigen in Art. 9 DS-GVO erwähnten, wenn sie mit besonderer Zweckbestimmung, nämlich zur eindeutigen Identifizierung und damit in besonders risikobehafteter Weise verarbeitet werden. Dieses erhöhte Risiko besteht nur dann, wenn automatisierte biometrische Erkennungsverfahren eingesetzt werden. Der in Art. 9 Abs. 1 DS-GVO verwendete Begriff der Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person entspricht dem der biometrischen Erkennung im international standardisierten biometrischen Vokabular.

Von einer biometrischen Erkennung kann nur bei einer automatisierten Erkennung die Rede sein, also bei einer Erkennung mittels eines rechnergestützten Systems. Eine manuelle Sichtkontrolle fiele nach diesem Verständnis aus dem in Art. 9 Abs. 1 DS-GVO verwendeten Begriff der Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person heraus.

Die biometrische Erkennung umfasst biometrische Verifikation und biometrische Identifikation. Die biometrische Verifikation meint nach dem international standardisierten biometrischen Vokabular den Prozess, in dem eine biometrische Behauptung durch einen biometrischen Vergleich bestätigt wird. Der Begriff der biometrischen Behauptung bezeichnet die Behauptung, dass eine zu erfassende betroffene Person die körperliche Quelle einer bestimmten biometrischen Referenz ist. Biometrische Referenz nennt man ein oder mehrere gespeicherte biometrische Samples, biometrische Templates oder biometrische Modelle, die einer betroffenen Person zugeordnet wurden und als Objekt zum biometrischen Vergleich verwendet werden. Die biometrische Referenz kann sich in einer Datenbank, verteilt in einem Netzwerk oder auf einer Smartcard befinden.

Als biometrische Identifikation wird der Prozess der Suche in einer biometrischen Enrolmentdatenbank nach dem Identifikator einer biometrischen Referenz, der einem einzigen Individuum zugeordnet werden kann, bezeichnet. Eine biometrische Enrolmentdatenbank besteht aus Datensätzen enrolter Personen, die nicht-biometrische Daten sowie Identifikatoren biometrischer Referenzen beinhalten. Als Identifikator einer biometrischen Referenz bezeichnet man den Zeiger auf einen biometrischen Referenzdatensatz in der biometrischen Referenzdatenbank. Ein Referenzdatensatz ist ein indexierter Datensatz, der biometrische Referenzen beinhaltet. Hierbei ist zu beachten, dass eine einzelne biometrische Referenz (z. B. ein auf einer Speicherkarte gespeicherter Fingerabdruck) in einigen Transaktionen als biometrische Enrolmentdatenbank betrachtet werden kann.

Während der Anwender bei der Verifikation dem biometrischen System seine Identität vorab bekannt gibt (z. B. die User-ID über Tastatur oder Karte) und das System das biometrische Merkmal dann nur noch mit dem einen zur User-ID passenden Referenzmerkmal vergleichen muss (1:1-Vergleich), wird bei der Identifikation das biometrische Merkmal mit allen im biometrischen System gespeicherten Referenzmerkmalen verglichen (1:n-Vergleich).[31]

Auch Erwägungsgrund 51 legt nahe, dass die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung gemäß Art. 9 Abs. 1 DS-GVO sowohl Verfahren zur Identifikation als auch zur Authentisierung umfasst. Die Verfahren unterscheiden sich nur in der Anzahl der zum Vergleich herangezogenen Referenzdatensätze: Bei der Authentisierung wird gegen genau einen Referenzdatensatz geprüft, bei der Identifikation gegen mehrere. Dem so gebrauchten Begriff der Authentisierung entspricht im biometrischen Standard-Vokabular der Begriff der biometrischen Verifikation.

Biometrische Daten fallen somit erst unter den Begriff der „besonderen Kategorien personenbezogener Daten“ gemäß Art. 9 Abs. 1 DS-GVO, wenn sie zur eindeutigen Identifizierung einer natürlichen Person, das heißt zum Zweck der automatisierten biometrischen Erkennung verarbeitet werden. In diesem Fall ist der Anwendungsbereich der oben genannten Regelung eröffnet.

6.2.2 Ausgewählte Ausnahmetatbestände des Art. 9 Abs. 2 DS-GVO

Nicht untersagt ist die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person in den Fällen des Art. 9 Abs. 2 DS-GVO.

6.2.2.1 Art. 9 Abs. 2 lit. a DS-GVO

Die betroffene Person hat in die Verarbeitung ihrer biometrischen Daten zur Identifizierung ausdrücklich eingewilligt. Die Einwilligung muss sich dabei explizit auf die Verwendung der biometrischen Daten beziehen. Es muss somit eine ausdrückliche Bezugnahme auf die Daten in der Einwilligung vorliegen. Dies setzt voraus, dass auf die Sensitivität der Daten gesondert hingewiesen wird[32]. Durch die DS-GVO werden sämtliche personenbezogenen Daten geschützt, die in Art. 9 Abs. 1 DS-GVO genannten jedoch in besonderer Weise. Durch die Hinweise soll der Betroffene in die Lage versetzt werden, zu entscheiden, dass er sich möglicherweise mit der Einwilligung in die Datenverarbeitung außerhalb dieses besonderen rechtlichen Schutzes befindet. Eine konkludente Einwilligung ist somit nicht möglich.

Es ist der konkrete Zweck der Datenverarbeitung zu nennen. Dies wäre gemäß Art. 9 Abs. 1 DS-GVO zumindest der Zweck der eindeutigen Identifizierung.

---

[31] BSI, Einführung in die technischen Grundlagen der biometrischen Authentisierung, S. 1, erhältlich unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.pdf

[32] Weichert in Kühling/Buchner, DS-GVO, Art. 9 Rn. 47

An das Erfordernis einer freiwilligen Einwilligung in die Verarbeitung biometrischer Daten sind besonders hohe Anforderungen zu stellen, wenn sie im Rahmen eines Abhängigkeitsverhältnisses, wie zum Beispiel im Beschäftigtenverhältnis, erteilt wird.

6.2.2.2 Art. 9 Abs. 2 lit. b DS-GVO

Die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann. Art. 9 Abs. 2 lit. b DS-GVO ist kein aus sich heraus anwendbarer eigenständiger Erlaubnistatbestand, sondern verlangt vielmehr, dass sich die Erforderlichkeit der Datenverarbeitung zu vorgenannten Zwecken aus einer gesonderten, konkreten unionsrechtlichen oder einzelstaatlichen Norm, wozu auch Betriebsvereinbarungen und Tarifverträge zählen, ergibt.[33]

Biometrische Daten können im betrieblichen Kontext bei der Zugangsberechtigung, der Authentisierung an IT Systemen oder bei der Einlasskontrolle zu besonders schützenswerten Bereichen zum Einsatz kommen. Das Erforderlichkeitsprinzip ist in diesem Bereich eng auszulegen[34].

6.2.2.3 Art. 9 Abs. 2 lit. e DS-GVO

Eine Verarbeitung sensibler Daten kann nach Art. 9 Abs. 2 lit. e DS-GVO ferner dann erlaubt sein, wenn die betroffene Person die Daten offensichtlich öffentlich gemacht hat. Unter Öffentlichkeit in diesem Sinne ist die Allgemeinheit, also ein individuell nicht bestimmbarer Personenkreis zu verstehen. Außerdem muss die „betroffene Person“ die sensiblen Daten „offensichtlich“ öffentlich gemacht haben. Dies setzt einen unzweideutigen, bewussten Willensakt voraus, der final auf die Entäußerung des Datums in die Öffentlichkeit in dem erläuterten Sinne gerichtet ist. Durch dieses Merkmal soll verhindert werden, dass ein Betroffener dadurch den besonderen Schutz verliert, dass ein Dritter dessen sensitive Daten in die Öffentlichkeit trägt, oder dass dies durch den Betroffenen selbst unbeabsichtigt geschieht[35].

Das bloße „Dasein“ im öffentlichen Raum fällt nicht unter den Begriff der Veröffentlichung in diesem Sinne. Denn der entäußernde Charakter eines Willensaktes, bestimmte Daten einem unbestimmten Personenkreis zugänglich zu machen, kann nicht mit dem Bewegen im öffentlichen Raum gleichgesetzt werden. Damit ist insbesondere ausgeschlossen, dass Bildaufnahmen von Personen im öffentlichen Raum getätigt werden, um diese mittels eines Gesichtserkennungsprogramms zu verarbeiten oder um Personen auf politischen Veranstaltungen im öffentlichen Raum zu registrieren[36].

6.2.2.4 Art. 9 Abs. 2 lit. f DS-GVO

Zulässig ist die Verarbeitung gemäß Art. 9 Abs. 2 lit. f DS-GVO auch dann, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Ansprüche im Sinne des lit. f müssen nicht rechtshängig sein, so dass auch der vor- und außergerichtliche Rechtsverkehr erfasst wird.[37]

6.2.2.5 Art. 9 Abs. 2 lit. g DS-GVO

Die Verarbeitung ist gemäß Art. 9 Abs. 2 lit. g DS-GVO auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats aus Gründen eines erheblichen öffentlichen Interesses erforderlich. Es handelt sich hier nicht um einen eigenen Erlaubnistatbestand, sondern um eine Öffnungsklausel. Es werden besonders schützenswerte Belange des Gemeinwohls, bzw. der Gemeinschaftsgüter erfasst. Das Gemeinwohlinteresse muss das Persönlichkeitsrecht der betroffenen Person überwiegen.

6.3 Anwendung des Art. 6 Abs. 1 DS-GVO

Zusätzlich zu den speziellen Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten sollen nach Erwägungsgrund 51 die allgemeinen Grundsätze und andere Bestimmungen der DS-GVO, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung gelten. Bei besonders schutzbedürftigen Daten ist die Eingriffsintensität regelmäßig

[33] Schulz, in: Gola, DS-GVO, Art. 9 Rn. 18
[34] Weichert in Kühling/Buchner, DS-GVO, Art. 9 Rn. 54
[35] Weichert in Kühling/Buchner, DS-GVO, Art. 9 Rn. 79
[36] Schiff, in: Ehmann/Selmayr, DS-GVO, Art. 4 Rn. 40, 41
[37] Schulz, in: Gola, DS-GVO, Art. 9 Rn. 27

höher, weshalb höhere Anforderungen an die Rechtfertigung des Eingriffs zu stellen sind. Dies hat zur Folge, dass Art. 9 DS-GVO den Art. 6 DS-GVO nicht verdrängt, sondern dass seine Voraussetzungen zusätzlich zu denen des Art. 6 DS-GVO vorliegen müssen.

Werden zudem biometrische Daten nicht zur eindeutigen Identifizierung einer natürlichen Person, sondern zu anderen Zwecken verarbeitet, ist Art. 6 Abs. 1 DS-GVO einschlägig. Danach ist die Verarbeitung von personenbezogenen Daten nur rechtmäßig, wenn mindestens eine der darin geregelten Bedingungen erfüllt ist.

6.3.1 Einwilligung in die Datenverarbeitung gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO

Die Verarbeitung ist gemäß Art. 6 Abs. 1 S. 1 lit. a DS-GVO rechtmäßig, wenn die betroffene Person ihre Einwilligung erteilt hat. Eine Einwilligung ist nur unter den Voraussetzungen der hinreichenden Information und Freiwilligkeit möglich. Besondere Konstellationen wie beispielsweise eine Einwilligung im arbeitsrechtlichen Kontext sind auch hier zu berücksichtigen.

6.3.2 Erforderlichkeit zur Erfüllung eines Vertrages oder eines vorvertraglichen Verhältnisses gem. Art. 6 Abs. 1 S. 1 lit. b DS-GVO

Die Verarbeitung ist gemäß Art. 6 Abs. 1 S. 1 lit. b DS-GVO rechtmäßig, wenn sie für die Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Neben der „Erfüllung“ sind die Vorbereitung und Anbahnung des Vertrages, dessen Durchführung sowie auch dessen Abwicklung insbesondere zur Erfüllung von Gewährleistungspflichten oder sekundären Leistungspflichten erfasst. Auch vorvertragliche Maßnahmen können eine Verarbeitung legitimieren, allerdings nur, wenn sie „auf Anfrage der betroffenen Person erfolgen“[38].

Für die Erfüllung eines Vertrags ist eine Verarbeitung nur dann erforderlich, wenn sie für die Vertragszwecke notwendig ist. Das ist etwa der Fall bei der Speicherung einer Iris-Abbildung zur Herstellung eines Deko-Objektes aus dieser Abbildung, der Mitteilung von Kreditkartendetails zur Abwicklung der Zahlung eines Online-Kaufs, der Anschrift des Kunden für die vertraglich bedingte Korrespondenz oder bei der Angabe der Bankverbindung für die Gehaltsüberweisung. Dagegen ist die Speicherung von Kundenpräferenzen für Marketingzwecke nicht für die Erfüllung des Vertrags erforderlich.[39]

6.3.3 Erforderlichkeit zur Wahrung der berechtigten Interessen des Verantwortlichen gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO

Die Verarbeitung ist gemäß Art. 6 Abs. 1 S. 1 lit. f DS-GVO rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Grundrechten und Grundfreiheiten der betroffenen Person überwiegen.

Die Datenverarbeitung muss im berechtigten Interesse des Verantwortlichen oder eines Dritten liegen. Das berechtigte Interesse kann rechtlicher, wirtschaftlicher oder ideeller Natur sein. In EG 47 sind Beispiele für das berechtigte Interesse aufgeführt. Dies sind die Verhinderung von Betrug und Zwecke der Direktwerbung. Zu bestimmen ist als erstes das Interesse der verantwortlichen Stelle auf Grundlage der Zweckbestimmung.

Die Verarbeitung muss ferner zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein.

Den berechtigten Interessen der Verantwortlichen Stelle dürfen keine überwiegenden Interessen oder Grundrechte oder Grundfreiheiten der betroffenen Person entgegenstehen.

Dabei sind die für beide Seiten bestimmten Interessen zu gewichten. Die zum bislang geltenden Recht entwickelten Faktoren der Gewichtung behalten dabei auch in Ansehung der DS-GVO ihre Gültigkeit, wobei künftig dem Ausfluss europäischer Grundfreiheiten und -rechte besondere Bedeutung zukommt.[40]

Als Abwägungskriterium kommt noch die vernünftige Erwartungshaltung der betroffenen Person hinzu (EG 47). Im Rahmen der Interessenabwägung ist somit zu berücksichtigen, ob eine betroffene Person

[38] Plath in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 6 DSGVO, Rn.10
[39] Heberlein, in: Ehmann/Selmayr, Art. 6 DS-GVO, Rn. 13
[40] Schulz, in: Gola, DS-GVO, Art. 6 Rn. 53

zum Zeitpunkt der Datenerhebung und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffen Person vernünftigerweise nicht mit der weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Personen überwiegen.[41]

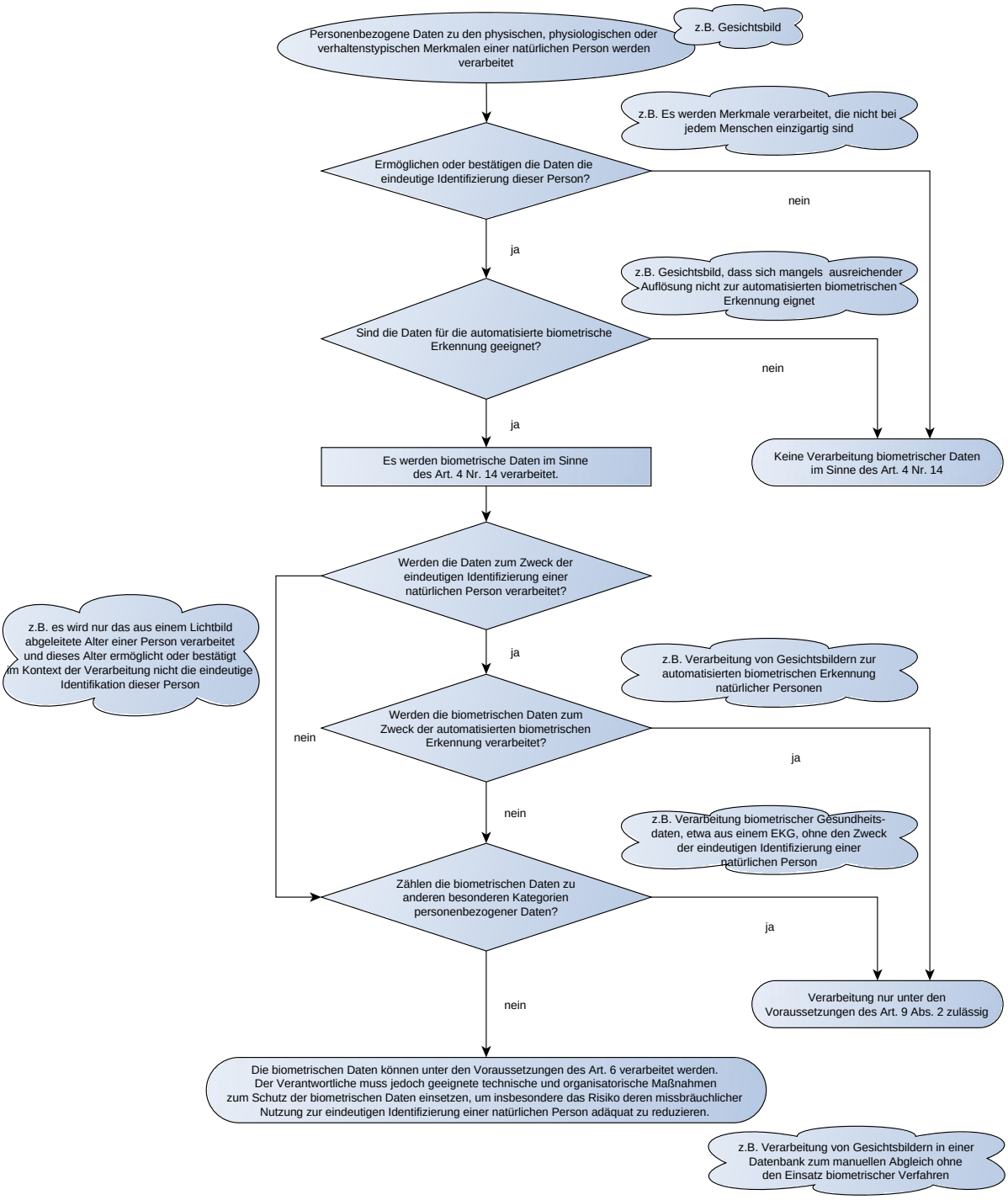


Abbildung 1 - Flussdiagram zur Klassifizierung von Verarbeitungen von Daten zu physischen, physiologischen oder verhaltenstypischen Merkmalen natürlicher Personen

41 Schulz in Gola, DS-GVO § 6 Rn. 55

6.4 Juristische Bewertung anhand ausgewählter Anwendungsfälle

6.4.1 Fall 1: Bezahlung des Schulessens mit Hilfe des Fingerabdrucks

Ein Unternehmen, das von einem Caterer zum Zwecke der Abrechnung der Mittagessen hinzugezogen wurde, bietet mehrere Methoden an, mit denen sich die Schulkinder bei der Mittagessensausgabe identifizieren können. Zu diesen Methoden gehört unter anderem die Identifikation mittels biometrischer Daten. Dabei wird der Fingerabdruck elektronisch eingelesen, gespeichert und zu Identifikationszwecken genutzt; das dabei erzeugte Template wird zur Identifikation innerhalb der jeweiligen Schülerschaft eingesetzt. Will sich ein Kind bei der Mittagessensausgabe identifizieren, so legt es seinen Finger auf, dabei wird erneut ein Template errechnet und mit den gespeicherten Templates verglichen. Liegt eine Übereinstimmung vor, so ist das Kind identifiziert, erhält das gebuchte Essen, und die finanzielle Abrechnung kann digital erfolgen.

Bei den verarbeiteten elektronischen Fingerabdrücken der Schüler handelt es sich um daktyloskopische und damit um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO. Diese werden auch im Sinne des Art. 9 Abs. 1 DS-GVO zum Zweck der eindeutigen Identifizierung der Schüler verarbeitet, da die ausgegebenen Essen zu Abrechnungszwecken bestimmten Schülern zugeordnet werden sollen. Als einzige Rechtsgrundlage für diese Verarbeitung kommt eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO in Betracht.

Die Einwilligung muss wirksam sein. Zu den Elementen einer wirksamen Einwilligung gehören Freiwilligkeit und Informiertheit. Solange ein Caterer mehrere gleichwertige und nicht-diskriminierende Methoden anbietet, mit deren Hilfe sich die Schüler bei der Essensausgabe identifizieren können, kann eine von den Eltern oder den einwilligungsfähigen Schülern erteilte Einwilligung in die Verarbeitung biometrischer Daten als „freiwillig“ angesehen werden. Angesichts der besonderen Schutzbedürftigkeit dieser Daten sind an die Freiwilligkeit – auch bei der angebotenen Alternative – strenge Maßstäbe anzulegen. Es muss sich um eine echte – und nicht nur formale – Alternative handeln, die z. B. nur in den AGB steht.

Auch an die Informiertheit müssen bei biometrischen Verfahren hohe Anforderungen gestellt werden. Da biometrische Daten als individuelle und universale Identifikatoren dienen können, ist die Bereitstellung klarer und leicht zugänglicher Informationen über die Nutzung der jeweiligen Daten als unabdingbare Voraussetzung für eine faire Verarbeitung zu betrachten. Wenn insbesondere der eingesetzte Algorithmus dasselbe biometrische Template auch in anderen biometrischen Systemen erzeugt, muss die betroffene Person wissen, dass sie auch in anderen biometrischen Systemen wiedererkannt werden kann.[42]

6.4.2 Fall 2: Zugang zu Firmenräumen mit Hilfe des Fingerabdrucks

Eine Firma, die im Internet mit Holzfenstern handelt und ungefähr 50 Mitarbeiter hat, plant den Einsatz eines biometrischen Zugangssystems mittels Fingerabdruck. Die Firma hat kein sicherheitsrelevantes Tätigkeitsgebiet; es besteht kein Unterschied zu anderen, „normalen“ Firmen. Der beabsichtigte Zweck (Zugangskontrolle) könnte auch mit einer Chipkarte, einem PIN-Code oder einem Passwort sichergestellt werden.

Bei den verarbeiteten elektronischen Fingerabdrücken der Mitarbeiter handelt es sich um daktyloskopische und damit um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO. Diese werden auch im Sinne des Art. 9 Abs. 1 DS-GVO zur eindeutigen Identifizierung der Mitarbeiter verarbeitet, da nur sie Zugang zu den Firmenräumen erhalten sollen. Als einzige Rechtsgrundlage für diese Verarbeitung kommt eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO in Betracht.

Um wirksam zu sein, muss die Einwilligung insbesondere freiwillig erfolgt sein. Nach Maßgabe des Erwägungsgrundes 43 ist eine Einwilligung dann nicht als freiwillig anzusehen, wenn ein klares Ungleichgewicht zwischen betroffener Person und dem Verantwortlichen der Datenverarbeitung besteht. Dies ist grundsätzlich im Rahmen von Arbeitsverhältnissen anzunehmen. Dennoch sind nach Ansicht des Europäischen Datenschutzausschusses auch im Rahmen von Arbeitsverhältnissen Situationen denkbar, in denen ein Arbeitgeber nachweisen kann, dass die Einwilligung in eine

[42] Artikel-29-Datenschutzgruppe, WP 193, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, S. 13.

Verarbeitung freiwillig erfolgte, insbesondere dann, wenn die Verweigerung der Einwilligung keinerlei nachteilige Folgen für den Arbeitnehmer gehabt hätte[43].

Auch nach § 26 Abs. 2 BDSG kann eine Verarbeitung personenbezogener Daten von Beschäftigten grundsätzlich auf der Grundlage einer Einwilligung erfolgen. Allerdings sind bei der Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann danach insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Weder das eine noch das andere ist hier jedoch der Fall.

Eine wirksame Einwilligung in die Verarbeitung daktyloskopischer und damit biometrischer Daten scheidet jedenfalls dann aus, wenn nicht alternativ die Verwendung anderer Mittel der Zugangskontrolle, wie Chipkarte, PIN-Code oder Passwort, angeboten wird.

6.4.3 Fall 3: Biometrischer Lichtbildabgleich durch Skiliftbetreiber

Die Kunden einer Skiliftanlage werden beim Betreten der Anlage fotografiert. Die so erhobenen Gesichtsbilder werden mit Referenzfotos, welche beim Kauf des Skipasses erstellt wurden, automatisiert abgeglichen. Zweck der Verarbeitung ist die Verhinderung von Leistungserschleichungen in Gestalt einer missbräuchlichen Verwendung des Skipasses durch unberechtigte Dritte, die den Skipass entweder nur ausgeliehen oder durch privaten, günstigeren Weiterverkauf erworben haben.

Bei den jeweils angefertigten Fotografien handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO sowie aufgrund der abgebildeten Gesichter um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO. Die Aufnahmen werden biometrisch abgeglichen, um die betroffene Person eindeutig zu identifizieren. Als mögliche Rechtsgrundlage kommt Art. 9 Abs. 2 lit. f DS-GVO in Betracht. Danach ist eine Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person zulässig, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, sei es in einem gerichtlichen oder einem außergerichtlichen Verfahren.

Es stellt sich die Frage, ob ein automatisierter Abgleich hier wirklich erforderlich ist. Dabei ist zu berücksichtigen, dass ein solcher Abgleich die Grundrechte und Grundfreiheiten der betroffenen Personen erheblich beeinträchtigt. Wenn auch vereinzelt Leistungserschleichungen in Gestalt einer missbräuchlichen Verwendung des Skipasses durch unberechtigte Dritte auftreten, so ist dennoch in der Regel davon auszugehen, dass sich die überwiegende Mehrheit der Kunden rechtstreu verhält, also für eine solche Art von Kontrollen keinerlei Anlass bietet, es sei denn, dass konkrete Umstände im Einzelfall (z. B. Nachweise über Missbräuche in nicht unerheblicher Zahl) die Erforderlichkeit einer solchen Maßnahme begründen können.

Vor diesem Hintergrund sollte dem Skiliftbetreiber die Durchführung etwa von Stichproben anhand der ausgegebenen Skipässe als milderes Mittel zuzumuten sein. Zu diesem Zweck kann der Skiliftbetreiber Skipässe verwenden, auf denen ab einer bestimmten Geltungsdauer ein Foto des Inhabers abgedruckt wird.

6.4.4 Fall 4: Zutrittskontrolle mit Handvenenscan für Flughafenmitarbeiter

Die F-GmbH betreibt zwei Flughäfen. Zur Sicherung des Flughafengeländes ist der Zugang zu den Sicherheitsbereichen nur berechtigten Personen gestattet. Die Zutrittsberechtigung wird durch die Vorlage des Flughafenausweises nachgewiesen. Darüber hinaus erfolgt eine zusätzliche biometrische Identitätsprüfung der Personen, die Zutritt zu den Sicherheitsbereichen des Flughafens haben, und zwar über das Verfahren der Handvenenbiometrie. Beim Einlesen der biometrischen Daten wird ein entsprechendes Handvenenmuster erstellt, welches auf dem Chip des Flughafenausweises in codierter Form hinterlegt wird. An den Kontrollstellen wird eine neue Handvenenaufnahme erstellt und mit der auf dem Chip des Ausweises gespeicherten Aufnahme verglichen. Der Handvenenscan bringe das derzeit höchste erreichbare Sicherheitsniveau bei der eindeutigen Identifizierung einer Person

[43] Artikel-29-Datenschutzgruppe, WP 259, Guidelines on Consent under Regulation 2016/679, S. 8. Der Europäische Datenschutzausschuss hat den auf die DS-GVO bezogenen Working Papers der Artikel-29-Datenschutzgruppe in seiner ersten Sitzung zugestimmt.

und sei auch als wirksame Abschreckung gegen jedweden Manipulationsversuch zu sehen, heißt es aus Flughafenkreisen.

Bei den Aufnahmen der Handvenenmuster handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO. Da diese für eine automatisierte biometrische Erkennung eingesetzt werden können, handelt es sich auch um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO.

Die Verarbeitung der Aufnahmen der Handvenenmuster erfolgt im Sinne des Art. 9 Abs. 1 DS-GVO zur eindeutigen Identifizierung einer natürlichen Person. Die Identität des Ausweisinhabers soll zusätzlich durch den Vergleich der Handvenenaufnahmen überprüft werden.

Als Rechtsgrundlage für dieses Verfahren könnte Art. 9 Abs. 2 lit. g DS-GVO herangezogen werden. Danach ist eine Verarbeitung biometrischer Daten dann nicht untersagt, wenn sie aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. An der Sicherheit des Flugverkehrs besteht ein erhebliches öffentliches Interesse.

Allerdings ist Art. 9 Abs. 2 lit. g DS-GVO kein eigenständiger Erlaubnistatbestand. Hinzutreten muss eine Rechtsgrundlage des Unionsrechts oder des Rechts eines Mitgliedstaats. In Betracht kommt hier § 8 Abs. 1 Nr. 4 Luftsicherheitsgesetz. Danach ist der Betreiber eines Flugplatzes zum Schutz des Flughafenbetriebs vor Angriffen auf die Sicherheit des Luftverkehrs verpflichtet, die Bereiche der Luftseite gegen unberechtigten Zugang zu sichern und, soweit es sich um Sicherheitsbereiche oder sensible Teile der Sicherheitsbereiche handelt, den Zugang nur hierzu besonders berechtigten Personen zu gestatten. Dem soll hier der Einsatz der Handvenenscanner dienen.

Die Verarbeitung muss allerdings zur Wahrung der Sicherheit des Flugverkehrs erforderlich sein. Zwar haben zwei Informatiker im Dezember 2018 gezeigt, wie sich Handvenenscangeräte überlisten lassen. Ein Einsatz dieser Technik unter organisatorisch abgesicherten Bedingungen und, wie hier, mit einer Zwei-Faktor-Authentisierung, wird vorliegend dennoch als zulässig erachtet, zumal gleich wirksame, aber mit Blick auf die informationelle Selbstbestimmung der betroffenen Personen weniger einschneidende Mittel wohl nicht zur Verfügung stehen.

6.4.5 Fall 5: Zielgerichtete Außenwerbung durch biometrische Gesichtsanalyse

Ein Unternehmen betreibt ein System zur Außenwerbung. Dieses ermöglicht mithilfe von Sensoren an Informationsbildschirmen, biometrische Merkmale von Umstehenden zu erfassen und Alter und Geschlecht dieser Personen zu analysieren. Das Produkt dient dazu, die auf dem Bildschirm ausgegebenen Werbebotschaften an Alter und Geschlecht der umstehenden Personen anzupassen. Die an einem Bildschirm angebrachten Kamerasensoren erkennen und erfassen zunächst das Gesicht der Betrachtenden. Diese Bilder werden als Videostream temporär in einem Zwischenspeicher der Kamera abgelegt, bevor die darin verbaute Software sie in Histogramme umwandelt. Die Kamera verfügt zudem über einen Kalibriermodus, der eine Visualisierung der aufgezeichneten Bilder ermöglicht. Sonstige Übertragungen der Bilddaten finden nicht statt, es besteht auch keine Zugriffsmöglichkeit auf Bilddaten für das Unternehmen, Werbevertragspartner oder Dritte.

***Abwandlung:** Ein Unternehmen vertreibt eine Software zur Außenwerbung. Der Lizenznehmer installiert die Software auf seiner Hardware und bringt über dem Werbebildschirm eine von ihm selbst anzuschaffende, handelsübliche Videokamera an. Diese sendet einen Videostream an den Computer, wo die Software die erfassten Gesichter (Blick Richtung Kamera) sowie deren Bewegungsrichtung auswertet. Sodann werden die erfassten Gesichter mit Hilfe eines Algorithmus anhand biometrischer Merkmale (z. B. Behaarung, stark ausgeprägter Adamsapfel, Falten) ausgewertet. Nachdem die aufgenommene Person das Kamerafeld verlassen hat, wird das Ergebnis dieser Auswertung in einem Log File festgehalten. Die sich im RAM befindlichen Bild-Informationen werden mit dessen Erstellung automatisch gelöscht.*

Bei den Videoaufnahmen handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO, auch wenn diese nur für einen sehr kurzen Zeitraum gespeichert werden.

Die Videoaufnahmen werden anhand biometrischer Merkmale ausgewertet. Allerdings erfolgt dies nicht zur eindeutigen Identifizierung der betroffenen Person, sondern vielmehr, um diese automatisch einer bestimmten Kategorie (u. a. Alter, Geschlecht) zuzuweisen. Die Rechtsgrundlage für diese Verarbeitung ist daher nicht in Art. 9 Abs. 2, sondern in Art. 6 Abs. 1 DS-GVO zu suchen.

Nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Der hier verfolgte Zweck der Direktwerbung kann als eine einem berechtigten Interesse im Sinne von Art. 6 Abs. 1 lit. f DS-GVO dienende Verarbeitung betrachtet werden. In gleicher Weise geeignete Mittel zur Erfassung der Zielgruppengerechtigkeit der ausgespielten Werbespots dürften in der hier gelieferten Genauigkeit nicht zur Verfügung stehen.

Bei der nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO erforderlichen Abwägung ist entscheidend, ob die von der jeweils spezifischen Verarbeitungssituation ausgehenden Gefahren so groß und die bei ihrer Verwirklichung eintretenden Nachteile so erheblich sind, dass die Interessen der betroffenen Personen gegenüber denen des Verantwortlichen Vorrang beanspruchen können.[44] Je stärker das Maß der Beeinträchtigung durch die jeweilige Datenverarbeitung ist, desto „schutzwürdiger" sind die Interessen der betroffenen Personen.[45]

Einerseits spricht insbesondere dafür, dass die schutzwürdigen Interessen der betroffenen Personen überwiegen, dass hier durch die kurzzeitige Aufnahme von Gesichtsbildern und die Erfassung einzelner biometrischer Charakteristika grundsätzlich biometrische Daten verarbeitet werden. Die Verarbeitung biometrischer Charakteristika der Gesichter von Personen birgt erhebliche Sicherheitsrisiken und gegebenenfalls sind von einer Kompromittierung dieser Daten betroffene Personen lebenslangen Folgen eines Identitätsdiebstahls ausgesetzt, weil diese Daten nicht veränderbar sind.

Andererseits erhebt die eingesetzte Software nicht im ausreichenden Umfang Daten, um dauerhaft eine eindeutige Identifizierung der betroffenen Personen zu ermöglichen. Außerdem ist das für die betroffenen Personen bestehende Risiko aufgrund der relativ geringen Speicherdauer eher gering. Das gilt allerdings nur dann, wenn der Speicherzeitraum nicht verlängert werden kann, eine Identifizierung (d.h. eine Wiedererkennbarkeit) und Profilbildung der betroffenen Personen ausgeschlossen ist, die eingesetzte Software nicht dahingehend manipuliert werden kann, dass Daten erhoben werden können, die eine eindeutige Identifizierung ermöglichen, und die tatsächlich stattfindende Datenverarbeitung und ihr Zweck hinreichend transparent gemacht werden (Art. 13 Abs. 1 DS-GVO).

Zur Abwandlung: Anders als im Ursprungsfall handelt es sich bei der Abwandlung nicht um ein geschlossenes System. Die in Gestalt der Videoaufnahmen erhobenen personenbezogenen Daten können länger gespeichert und zu anderen Zwecken, etwa zur eindeutigen Identifizierung der betroffenen Personen, weiterverwendet werden. Damit bewegen sich die in diesem Fall ergriffenen technischen und organisatorischen Maßnahmen auf einem deutlich niedrigeren Niveau, so dass im Ergebnis die Interessen der betroffenen Personen hier überwiegen. Die Voraussetzungen des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO sind daher nicht erfüllt.

6.4.6 Fall 6: Zugangskontrolle auf Kreuzfahrtschiff

Auf einem Kreuzfahrtschiff wird beim Einchecken ein Foto angefertigt und gespeichert. Bei jedem Verlassen und Betreten des Schiffes wird die Chipkarte ausgelesen und der Fahrgast anhand des im System gespeicherten Fotos kontrolliert.

Wenn auf einem digitalen Bild gut erkennbar das Gesicht einer Person abgebildet ist, handelt es sich dabei um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO und zugleich um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO, da es für eine automatisierte biometrische Erkennung eingesetzt werden kann.

Eine Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person im Sinne des Art. 9 Abs. 1 DS-GVO liegt hier jedoch nicht vor. Die Bilder werden nicht zum Zweck der automatisierten biometrischen Erkennung verarbeitet, sondern sollen bei einem manuellen Bildabgleich zum Einsatz kommen.

Als Rechtsgrundlage für die Verarbeitung kommt somit Art. 6 Abs. 1 lit. f DS-GVO in Betracht. Der Reeder hat ein berechtigtes Interesse daran, dass nur Fahrgäste das Kreuzfahrtschiff betreten. Die Kontrolle beim Verlassen des Schiffes verschafft der Besatzung einen Überblick darüber, wer sich auf

[44] Scholz, in Simitis, BDSG, § 6b Rn. 93.
[45] Scholz, a.a.O., Rn. 94.

Landgang befindet. Beides entspricht auch dem Interesse der Fahrgäste, so dass die Verarbeitung als zulässig angesehen werden kann.

6.4.7 Fall 7: Videokamera in Juweliergeschäft

Der Inhaber eines Juweliergeschäfts installiert eine Videokamera und speichert die Aufnahmen für 48 Stunden. Er besitzt keine Software zur Gesichtserkennung, beabsichtigt aber im Falle einer Straftat die Weitergabe von Videoaufnahmen an die Polizei zum Zwecke der Identifikation von potentiellen Straftätern, durch manuellen Bildvergleich und gegebenenfalls durch biometrische Verfahren.

Bei den Videoaufnahmen handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO. Videoaufnahmen insbesondere von Gesichtern können je nach Funktionalität der technischen Anlage grundsätzlich für eine Auswertung (z. B. Identifikation) anhand biometrischer Merkmale geeignet sein. Sie enthalten dann alle Informationen, die für eine solche Auswertung relevant sind.

Solche Videoaufnahmen sind daher als biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO einzustufen. Untersagt ist nach Art. 9 Abs. 1 DS-GVO lediglich eine Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person, also zum Zweck der automatisierten biometrischen Erkennung.

Eine solche Verarbeitung findet hier jedoch nicht statt, da der Juwelier nicht über ein biometrisches Identifikationssystem verfügt. Darunter versteht man ein System zum Zwecke der biometrischen Erkennung von Individuen anhand ihres Verhaltens oder ihren biologischen Charakteristika.[46]

Auch ist zu bedenken, dass es nicht Sache des Juweliers ist, potentielle Straftäter zu identifizieren. Dies ist die Aufgabe von Polizei und Staatsanwaltschaft. Ihnen übergibt der Juwelier im Falle einer Straftat die Aufnahmen zur näheren Auswertung.

Als Rechtsgrundlage in Betracht kommt hier daher Art. 6 Abs. 1 S. 1 lit. f DS-GVO. Es kann dahingestellt bleiben, ob bei der Videoüberwachung durch Privatpersonen § 4 BDSG oder Art. 6 Abs. 1 S. 1 lit. f DS-GVO zur Anwendung kommt, da beide Vorschriften in vielen Fällen zu gleichen Ergebnissen führen. Nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Die verfolgten Zwecke der Verhinderung von Straftaten einerseits sowie der Überführung von Straftätern andererseits können als berechtigte Interessen im Sinne des Art. 6 Abs. 1 S. 1 lit. f DS-GVO angesehen werden. Gleich wirksame, aber mit Blick auf die informationelle Selbstbestimmung der betroffenen Personen weniger einschneidende Mittel stehen wohl nicht zur Verfügung.

Bei der nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO erforderlichen Abwägung ist entscheidend, ob die von der jeweils spezifischen Verarbeitungssituation ausgehenden Gefahren so groß und die bei ihrer Verwirklichung eintretenden Nachteile so erheblich sind, dass die Interessen der betroffenen Personen gegenüber denen des Verantwortlichen Vorrang beanspruchen können.[47] Je stärker das Maß der Beeinträchtigung durch die jeweilige Datenverarbeitung ist, desto „schutzwürdiger“ sind die Interessen der betroffenen Personen.[48]

Dafür, dass die schutzwürdigen Interessen der betroffenen Personen überwiegen, spricht die hier erfolgende Aufnahme und Speicherung von Gesichtsbildern sowie deren grundsätzliche Eignung zur eindeutigen Identifizierung natürlicher Personen. Die sich daraus ergebenden Risiken für die Rechte und Freiheiten der betroffenen Personen muss der Verantwortliche durch technische und organisatorische Maßnahmen minimieren. Zu Gunsten des Verantwortlichen kann die Abwägung jedoch nur dann ausgehen, wenn er sicherstellt, dass eine Speicherdauer von 48 bis maximal 72 Stunden nicht überschritten wird, dass auf seiner Hardware keine Gesichtserkennungssoftware installiert und genutzt wird und dass die stattfindende Datenverarbeitung sowie deren Zwecke den betroffenen Personen hinreichend transparent gemacht werden (Art. 13 Abs. 1 DS-GVO).

---

[46] ISO/IEC JTC SC37 Harmonized Biometric Vocabulary (HBV) as defined in SC37 Working Group 1 for the International Standard ISO/IEC 2382-37

[47] Scholz, a.a.O., Rn. 93.

[48] Scholz, a.a.O., Rn. 94.

6.4.8 Fall 8: VIP-Gast-Erkennung in Hotels

Ein Hotel benutzt eine Videoüberwachungsanlage mit Gesichtserkennungssystem, das den Hotel Manager auf angekommene VIP-Gäste aufmerksam macht. Aufnahmen dieser VIP-Gäste wurden zuvor mit deren Einverständnis in eine Datenbank aufgenommen. Allerdings werden auch von allen anderen Gästen Videoaufnahmen gemacht, Templates erstellt und mit dem Inhalt der Datenbank verglichen.

Wenn auf einem digitalen Bild klar sichtbar das Gesicht einer Person abgebildet ist, handelt es sich dabei um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO. Die hier mit Hilfe der Videoüberwachungsanlage verarbeiteten Gesichtsbilder sind zudem als biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO einzustufen, da sie für eine automatisierte biometrische Erkennung eingesetzt werden können.

Die Verarbeitung der Videoaufnahmen erfolgt auch zum Zwecke der eindeutigen Identifizierung einer natürlichen Person im Sinne des Art. 9 Abs. 1 DS-GVO. Der Hotel Manager möchte auf angekommene VIP-Gäste aufmerksam gemacht werden, diese namentlich ansprechen können und von nicht als VIPs eingestuften Gästen unterscheiden.

Die Verarbeitung betrifft alle Personen, die den Eingangsbereich des Hotels betreten, also als VIPs registrierte und nicht registrierte Gäste. Zweck der Verarbeitung ist eine biometrische Erkennung. Von allen Gästen werden digitale Gesichtsbilder erstellt. Aus den Gesichtsbildern werden biometrische Merkmale extrahiert und mit den in der hoteleigenen Datenbank vorhandenen Daten verglichen. Darauf, ob sich als Ergebnis dieses Vergleichs ein Trefferfall ergibt oder nicht, kommt es für den Zweck der Verarbeitung nicht an. Theoretisch kann jede Person, die den Eingangsbereich des Hotels betritt, ein VIP-Gast sein. Die Einbeziehung der Daten auch von Personen, deren Vergleich letztlich zu Nichttreffern führt, ist notwendiger und gewollter Teil des Verfahrens und gibt diesem erst seinen Sinn.

Für die Verarbeitung der Gesichtsbilder der bereits als VIPs registrierten Gäste kann gemäß Art. 9 Abs. 2 lit. a DS-GVO deren ausdrückliche Einwilligung herangezogen werden. Für die Verarbeitung der Gesichtsbilder der anderen Gäste ist eine Rechtsgrundlage nicht ersichtlich. In seiner derzeitigen Gestalt lässt sich das Verfahren somit nicht in Einklang mit der DS-GVO bringen.

7 Auswahl von Maßnahmen und Schlussfolgerungen für die Verfahrensgestaltung

7.1 Modell und Grundannahmen

7.1.1 Methodik

Da die Verarbeitung personenbezogener Daten immer ein Risiko für die Rechte und Freiheiten betroffener Personen darstellt, sind die Verantwortlichen dazu verpflichtet, die Grundsätze aus Art. 5 DS-GVO einhalten. Die getroffenen Maßnahmen sind nach Art. 5 Abs. 2 DS-GVO zu dokumentieren. Die Nicht-Einhaltung der in Art. 5 verankerten Grundsätze kann gemäß Art. 83 Abs. 5 lit. a DS-GVO mit einem Bußgeld geahndet werden.

Um diese Grundsätze einhalten zu können, müssen gemäß Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Verantwortliche und Auftragsverarbeiter haben die jeweiligen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen auszuwählen. Biometrische Daten erfordern in aller Regel eine besondere Aufmerksamkeit, da eine Einzelperson unwiderruflich mit ihnen verbunden ist und anhand dieser Daten aufgrund ihrer individuellen verhaltensbezogenen oder physiologischen Merkmale zweifelsfrei identifiziert werden kann.

Das von den unabhängigen Datenschutzbehörden des Bundes und der Länder entwickelte Standard-Datenschutzmodell (SDM) bietet geeignete Hilfestellungen, um die rechtlichen Anforderungen der DS-GVO in konkrete technische und organisatorische Maßnahmen zu überführen, auch wenn die Arbeit an einzelnen Teilen derzeit noch nicht abgeschlossen ist. Das SDM strukturiert die rechtlichen Anforderungen in Form der folgenden Gewährleistungsziele: Datenminimierung, Verfügbarkeit,

Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit. Diese Anforderungen zielen auf Eigenschaften einer rechtskonformen Verarbeitung, die durch technische und organisatorische Maßnahmen „gewährleistet“ werden müssen. Die Gewährleistung besteht im Ausschluss von Abweichungen von einer rechtskonformen Verarbeitung Durch diese Gewährleistungsziele werden die rechtlichen Anforderungen der DS-GVO in die von der Verordnung geforderten technischen und organisatorischen Maßnahmen überführt. Das SDM enthält eine Auflistung generischer technischer und organisatorischer Maßnahmen. Mit Hilfe dieses generischen Katalogs kann bei jeder einzelnen Verarbeitung sowohl durch den Verantwortlichen selbst als auch durch die Aufsichtsbehörde geprüft werden, ob die vor Ort vorhandenen Maßnahmen das rechtlich geforderte Soll von Maßnahmen erfüllen.[49]

Wegen der Vielfalt der betrachteten Systeme ist eine vollständige und detaillierte Darstellung der Risiken und angemessenen zu ergreifenden technischen und organisatorischen Maßnahmen im Rahmen des vorliegenden Papiers nicht möglich. Um die Grundsätze der Datenverarbeitung gemäß Art. 5 DS-GVO einhalten zu können, müssen Verantwortliche ihre Systeme individuell untersuchen.

7.1.2 Systemaufbau

In einem ersten Schritt ist zunächst das zur Anwendung kommende System zu analysieren. Die Untersuchung eines Systems erfordert zunächst die Bestimmung der Systemgrenzen und der grundlegenden Struktur des Systems. Systeme zur Verarbeitung biometrischer Daten, wie sie im vorliegenden Papier vorgestellt werden, bestehen typischer Weise aus den folgenden Komponenten:

- Biometrische Erfassungsgeräte
- Verarbeitungslogik (führt insbesondere die biometrische Merkmalsextraktion und die biometrische Erkennung durch)
- Aktor(en): (an die Verarbeitungslogik angeschlossene Ausgabegeräte)
- Referenzdatenbank, Enrolmentdatenbank
- Weitere Eingabeschnittstellen
- Weitere Ausgabeschnittstellen
- Wartungsschnittstellen
- Verbindungen zwischen den Komponenten

Sodann sind die an der Verarbeitung beteiligten Akteure zu identifizieren. Akteure, die einen Einfluss auf die Verarbeitung der Daten im System haben oder haben können, sind in der Regel:

- Systembetreiber
- Betroffene
- Wartungsunternehmen
- Hersteller
- ggf. Stellen, die dem System Daten zur Verfügung stellen oder Daten aus ihm erhalten.

Daneben müssen auch solche Akteure betrachtet werden, die ein Interesse an einer nicht bestimmungsgemäßen Verarbeitung von Daten in oder aus dem System haben könnten. Dies ist erforderlich, um prüfen zu können, ob die Sicherheitsmaßnahmen, die der Verantwortliche ergriffen hat, die Betroffenen auch hinreichend stark gegen Missbrauch schützen. Hierbei werden sowohl persönliche, als auch wirtschaftliche oder politische Motive zu berücksichtigen sein. Abbildung 2 – Überblick über typische Komponenten biometrischer Systeme zeigt die Akteure und Komponenten biometrischer Systeme und ihre Verbindungen.

[49] Standard-Datenschutzmodell (SDM), Version 1.1, verabschiedet von der 95. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 26. April 2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf, S. 5.

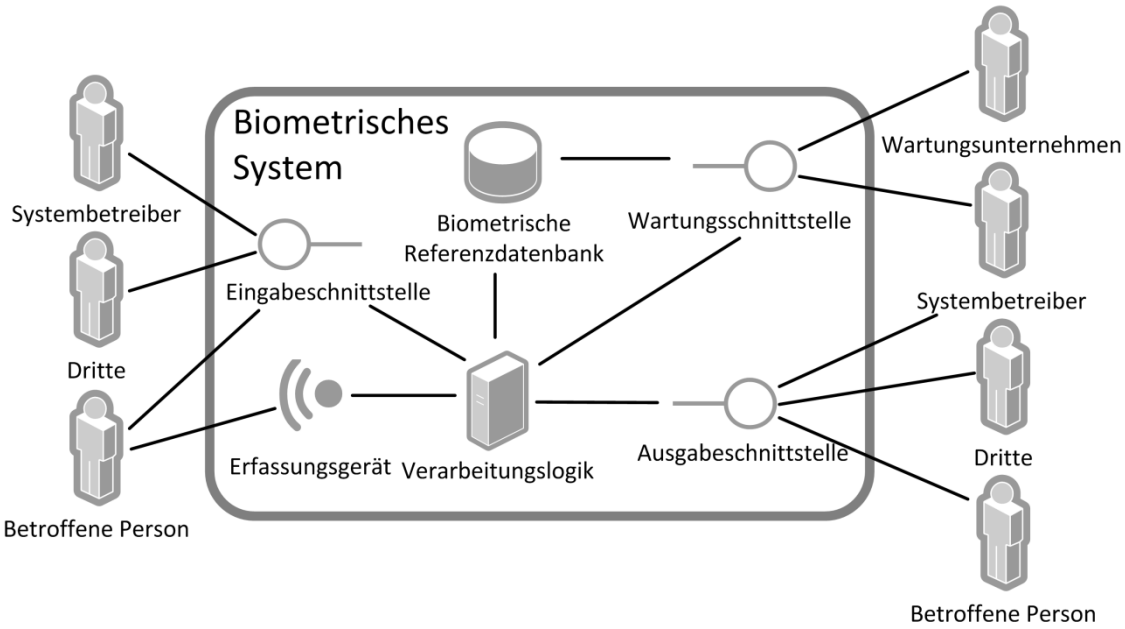


Abbildung 2 – Überblick über typische Komponenten biometrischer Systeme

Nicht in allen Systemen findet sich jede der genannten Komponenten. So entfällt die Referenzdatenbank bei der Reichweitenmessung und in Authentifizierungsverfahren kann die Referenzdatenbank auf einen Datensatz beschränkt sein, wenn beispielsweise die Identität einer Person ausschließlich anhand der in einem Ausweisdokument gespeicherten Daten überprüft wird. Die Wartungsschnittstelle wird hingegen in der Regel zu berücksichtigen sein: Eingebettete Systeme enthalten eine solche Schnittstelle zu Zwecken der Programmierung und der Diagnose; auf offenen Systemen wie PC-Technik basierte Lösungen gestatten problemlos den Einsatz von Fernwartungstechnik oder haben entsprechende Komponenten bereits vorinstalliert.

7.1.3 Überblick über die für biometrische Systeme typischen Verarbeitungen

Gemäß der zuvor betrachteten biometrischen Systeme und Fallbeispiele können im Wesentlichen drei Arten von biometrischen Systemen unterschieden werden, die jeweils unterschiedliche Risiken für die Rechte und Freiheiten Betroffener mit sich bringen:

- Systeme zur biometrischen Suche,
- Systeme zum biometrischen Vergleich oder
- Systeme zur biometrischen Eigenschaftsableitung.

Derzeit haben praktisch relevante biometrischen Systeme gemein, dass eine Erfassung biometrischer Charakteristika betroffener Personen in der Form biometrischer Sample erfolgt und aus diesen biometrische Merkmale extrahiert werden. Verfahren zur biometrischen Suche bedürfen darüber hinaus, dass biometrische Daten in einer Datenbank (in der Regel zusammen mit zusätzlichen Daten) erfasst werden, das sogenannte Enrolment. Somit können im Wesentlichen sechs verschiedene Arten von Verarbeitungen differenziert werden (Erfassung, Merkmalsextraktion, Enrolment, Suche, Vergleich und Eigenschaftsableitung).

Bei der biometrischen Erfassung nimmt ein biometrisches Erfassungsgerät ein biometrisches Charakteristikum einer betroffenen Person in Form eines biometrischen Samples auf.

Zur weiteren Verarbeitung der aufgenommenen biometrischen Samples müssen aus diesen biometrische Merkmale extrahiert werden. Abhängig davon, ob das biometrische System biometrische Merkmale oder biometrische Samples verwendet, erfolgt dieser Verarbeitungsschritt direkt nach der biometrischen Erfassung oder die Merkmalsextraktion ist Teil der Verarbeitungslogik (Enrolment, Suche, Vergleich, oder Eigenschaftsableitung).

Beim Enrolment wird eine biometrische Probe (Sample oder Merkmal) als biometrische Referenz zusammen mit weiteren Daten der betroffenen Person, die über eine entsprechende Eingabeschnittstelle erhoben werden, in einer biometrischen Referenzdatenbank gespeichert.

Bei der biometrischen Suche wird geprüft, ob eine gegebene biometrische Probe mit biometrischen Referenzen in der biometrischen Referenzdatenbank übereinstimmt und es wird eine Liste möglicher Kandidaten an eine Ausgabeschnittstelle gegeben.

Im Vergleich zur biometrischen Suche wird beim biometrischen Vergleich lediglich geprüft, zu welchem Grad eine gegebene biometrische Probe mit einer biometrischen Referenz übereinstimmt und der entsprechende Vergleichswert wird an eine Ausgabeschnittstelle weitergeleitet.

Bei der biometrischen Eigenschaftsableitung werden aus einem biometrischen Sample biometrische Eigenschaften berechnet und an eine Ausgabeschnittstelle weitergegeben. Die biometrischen Samples können dabei von einem biometrischen Erfassungsgerät, über eine Eingabeschnittstelle, oder aus einer biometrischen Referenzdatenbank stammen.

Sollten zukünftige Verfahren, die, beispielsweise unterstützt durch Künstliche Intelligenz, auf eine andere Art eine biometrische Erkennung durchführen, müssten die dabei durchgeführten Verarbeitungsschritte nach den Vorgaben dieses Papiers gesondert betrachtet werden.

7.2 Risiken

Um ein angemessenes Schutzniveau gewährleisten zu können, muss der Verantwortliche die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen identifizieren.

Der Begriff des Risikos ist in der DS-GVO nicht ausdrücklich definiert. Aus den Erwägungsgründen 75 und 94 Satz 2 DS-GVO kann folgende Definition hergeleitet werden: Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich einer ungerechtfertigten Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.[50]

Die DS-GVO gibt dem Verantwortlichen im Erwägungsgrund 76 zwei Stufen zur Bestimmung des Risikos einer personenbezogenen Verarbeitungstätigkeit vor, nämlich "Risiken" und "hohe Risiken". Zur Feststellung der Risikostufe ist die Art, der Umfang, die Umstände und die Zwecke der Verarbeitungstätigkeit sowie die spezifischen Eintrittswahrscheinlichkeiten und Schwere der Risiken bei der jeweiligen Verarbeitungstätigkeit zu berücksichtigen.

Speziell bei der Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person müssen die spezifischen Risiken betrachtet werden, die sich allein aus diesem Umstand ergeben.[51] Zur Identifikation von Datenschutzrisiken bietet es sich an, von folgenden Fragen auszugehen:

- Welche Schäden können für die natürlichen Personen auf der Grundlage der zu verarbeitenden Daten entstehen?
- Wodurch, d. h. durch welche Ereignisse kann es zu einem Schaden kommen?
- Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?[52]

In den hier betrachteten Verfahren werden überwiegend biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person im Sinne des Art. 9 Abs. 1 DS-GVO verarbeitet. Ungeachtet der Eintrittswahrscheinlichkeit eines möglichen Schadens kann zumindest regelmäßig von einer besonderen Schwere des Schadens ausgegangen werden. Dies ergibt sich bereits aus dem Umstand, dass es sich teilweise um die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO handelt, bei denen die DS-GVO einen gesteigerten Schutzbedarf vorsieht. Der Schaden dürfte außerdem nicht oder kaum reversibel sein, da die Identität einer natürlichen Person, wie eingangs bereits erwähnt, unwiderruflich und untrennbar mit ihren biometrischen Daten verbunden ist. Die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung natürlicher Personen ist daher ein wichtiges Indiz für ein „hohes Risiko“ im Sinne des

[50] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, S. 1.

[51] Europäischer Datenschutzausschuss: Working Paper 193 „Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien“, S. 5

[52] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, S. 2.

Erwägungsgrundes 76.[53] Das Kurzpapier Nr. 18 der DSK zum Thema „Risiko für die Rechte und Freiheiten natürlicher Personen“ bietet für die Abschätzung des Risikos eine Matrix an, die Verantwortliche zur Feststellung des Risikos bei der von ihnen beabsichtigten Verarbeitungstätigkeit heranziehen können. Sollten Verantwortliche zu dem Ergebnis kommen, dass die von ihnen beabsichtigte Verarbeitungstätigkeit voraussichtlich ein „hohes Risiko“ für die Rechte und Freiheiten natürlicher Personen darstellt, ist die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO notwendig.

7.3 Maßnahmen

Folgt man der Systematik des Standard-Datenschutzmodells, müssen die eingangs erwähnten Gewährleistungsziele (Sicherung der Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit) auch bei der Verarbeitung biometrischer Daten bzw. bei der Nutzung biometrischer Verfahren erreicht werden. Dabei sind die spezifischen Risiken, die mit dem Einsatz biometrischer Verfahren und der Verarbeitung biometrischer Daten verbunden sind, zu berücksichtigen. Jedes der Gewährleistungsziele kann durch bestimmte technische und organisatorische Maßnahmen erreicht werden, die im Standard-Datenschutzmodell zumindest in generischer Form beschrieben sind.[54] Neben den im SDM verschriftlichten generischen Maßnahmen zur Umsetzung der Gewährleistungsziele ist eine weitere Komponente zu beachten, sofern für eine beabsichtigte Verarbeitungstätigkeit ein „hohes Risiko“ für die Rechte und Freiheiten der betroffenen Personen festgestellt wurde. Ein „hohes Risiko“ entspricht einem „hohen Schutzbedarf“ und führt zu Maßnahmen mit entsprechend höheren Anforderungen an deren Wirksamkeit oder erfordert sogar zusätzliche Maßnahmen.[55] Konkret bedeutet dies, dass jede der getroffenen Schutzmaßnahme wiederum selbst anhand der Gewährleistungsziele beurteilt werden muss. Wenn z. B. das Gewährleistungsziel „Vertraulichkeit“ in einem biometrischen System erreicht werden soll, indem ein Rechte- und Rollenkonzept nach dem Erforderlichkeitsprinzip festgelegt wird, so muss dieses Rechte- und Rollenkonzept selbst verfügbar, integer, vertraulich, nichtverkettbar, transparent und intervenierbar sein. Oder, um noch ein weiteres Beispiel zu nennen: Bei hohem Risiko reicht es nicht, Aktivitäten des Systems zu protokollieren, die Protokolldaten müssen ihrerseits verfügbar sein, die Revisionsfestigkeit kann z. B. durch die Verwendung von Signaturen gesichert werden, es gilt zu überlegen, ob Protokolldaten nur verschlüsselt gespeichert werden usw. Entscheidend ist zudem, dass bei hohen Risiken nach dem SDM ein Datenschutzmanagement-System zu betreiben ist, das dafür sorgt, dass festgestellte Schwächen und Mängel auch nachhaltig behoben werden können.

7.4 Restrisiko

Nach der Auswahl von technischen und organisatorischen Maßnahmen und deren Umsetzung muss das verbleibende Risiko für die betroffenen Personen beurteilt werden. Ergibt sich nach Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO ein hohes Restrisiko, muss die zuständige Aufsichtsbehörde konsultiert werden (Art. 36 DS-GVO).[56]

[53] Siehe auch: Europäischer Datenschutzausschuss: Working Paper 248 „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA)“

[54] Standard-Datenschutzmodell (SDM), Version 1.1, verabschiedet von der 95. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 26. April 2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf, S.22 ff.

[55] Standard-Datenschutzmodell (SDM), Version 1.1, verabschiedet von der 95. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 26. April 2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf, S.32.

[56] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, S. 6