Die Vermessung des Arbeitnehmers

Stephan Schindler · Thilo Goeble · Jana Schneider

Universität Kassel
{stephan.schindler | thilo.goeble | jana.schneider}@uni-kassel.de

Zusammenfassung

Die seit dem 25. Mai 2018 unmittelbar geltende europäische Datenschutz-Grundverordnung (DS-GVO; Artikelangaben ohne Bezeichnung beziehen sich auf diese) ersetzt die bestehenden Regelungen zum Datenschutz. Ergänzt wird die Verordnung durch das neue Bundesdatenschutzgesetz (BDSG). Zwar ist die Verarbeitung biometrischer Daten auch nach dem neuen Datenschutzrecht in ausgewählten Fällen erlaubt, dem sind jedoch enge Grenzen gesetzt. Überdies verpflichtet die DS-GVO zum Datenschutz durch Technikgestaltung. Es stellt sich daher die Frage, ob Unternehmen in Zukunft überhaupt noch biometrische Erkennung einsetzen dürfen und wie derartige Verfahren technisch auszugestalten sind. Dem soll am Beispiel von denkbaren Industrie 4.0-Anwendungen nachgegangen werden.

1 Biometrische Erkennung

Biometrie (griechisch: bios – Leben; métron – Maß) bezeichnet die Lehre von der Messung an Lebewesen. In einem engeren Sinn ist Biometrie als die (teil-)automatisierte Messung hoch spezifischer körperlicher oder verhaltenstypischer Merkmale zur Erkennung und Unterscheidung von Personen zu verstehen (im Folgenden: biometrische Erkennung) [JaRN11]. Dies betrifft z.B. die biometrische Gesichts-, Iris- sowie Fingerabdruckerkennung.

Biometrische Erkennung kann überall dort eingesetzt werden, wo es eine Person zu identifizieren oder eine vorgegebene Identität zu verifizieren gilt (z.B. bei der Zugangssicherung). Anders als bei einer Identitäts- und Berechtigungsprüfung basierend auf Besitz (z.B. Chipkarte) oder Wissen (z.B. PIN), können biometrische Merkmale grundsätzlich nicht verloren gehen oder weitergegeben werden. Dies verspricht ein Mehr an Sicherheit [JaRN11].

Biometrische Erkennung birgt aber auch Risiken. Aufgrund ihrer körperlichen (u.U. lebenslangen) Bindung an eine bestimmte Person eignet sie sich gut zur Überwachung sowie zur Erstellung von Persönlichkeitsprofilen. Überdies besteht die Gefahr, dass die biometrischen Informationen entwendet und zur Vorspiegelung einer falschen Identität genutzt werden (sog. Identitätsdiebstahl) [BBB+08] [HoSt05].

Körperliche Messungen müssen aber nicht immer mit dem Ziel biometrischer Erkennung erfolgen. Zur ergonomischen Gestaltung von Arbeitsplätzen oder zum Arbeitsschutz (z.B. zur Bestimmung des Sicherheitsabstandes zu einem autonom arbeitenden Roboter) genügt die Ermittlung von Maßen des menschlichen Körpers, etwa der Arm- und Beinlänge (sog. anthropometrische Messungen [Hofm16]), oder der Position eines menschlichen Körpers im Raum, ohne dass damit die Erkennung einer bestimmten Person verbunden sein muss.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 252-263.

2 Anwendungsszenarien in der Industrie 4.0

Industrie 4.0 bezeichnet die Digitalisierung und Automatisierung industrieller Prozesse, um eine flexible, individuelle und störungsresistente sowie ressourcenschonende Produktion zu ermöglichen. Die beständige Verfügbarkeit von Informationen soll Entscheidungen erleichtern und ein dezentraler Steuerungsansatz bei der Beherrschung zunehmend komplexerer Produktionsansätze helfen [HoHo17a] [ReZü17].

In diesem Kontext kann der Einsatz biometrischer Erkennung sowie sonstiger körperlicher Messungen helfen, Arbeitsabläufe effizienter und sicherer zu gestalten. Zunächst ist an den Einsatz biometrischer Erkennung überall dort zu denken, wo Arbeitnehmer identifiziert oder authentifiziert werden sollen, etwa im Bereich der Zutritts- und Zugangskontrolle (z.B. zu Gebäuden oder Arbeitscomputern) sowie zur Arbeitszeiterfassung [PrBj08].

Darüber hinaus existieren im Kontext der Industrie 4.0 unterschiedliche Anwendungsmöglichkeiten biometrischer Erkennung und sonstiger körperlicher Messungen. Dies betrifft zunächst die Individualisierung des Arbeitsplatzes. Die Erkennung des Arbeitnehmers kann z.B. die Einstellung des Arbeitstisches auf eine vorab festgelegte Höhe oder die Bereitstellung von Informationen, die auf den individuellen Lern- und Erfahrungsstand abgestimmt sind, ermöglichen. Weiterhin können derartige Verfahren helfen, Betriebsabläufe zu steuern, um eine optimale Auslastung des Betriebes zu erreichen. Dies gilt z.B. für die Lokalisierung des Arbeitnehmers auf dem Fabrikgelände oder die Erkennung von fehlerhaften Bewegungsabläufen (bspw. bei einer Reparatur) mit anschließender Warnung [Hofm16]. Des Weiteren kann auch der physische und psychische Zustand (freshness-Level) herangezogen werden, um die jeweilige Tätigkeit anzupassen, damit die Gesundheit des Arbeitnehmers geschützt wird. Schließlich kann die Erkennung menschlicher Körper bei der Zusammenarbeit mit intelligenten Robotern (Mensch-Roboter-Kollaboration) verhindern, dass Arbeitnehmer z.B. durch plötzlich ausschwenkende Roboterarme verletzt werden. Auch können Werkstücke von einem Roboter ergonomisch optimal positioniert werden [Hofm16].

In den genannten Beispielen ist freilich nicht immer eine biometrische Erkennung erforderlich. So kann die Erkennung des Arbeitnehmers zur Individualisierung des Arbeitsplatzes auch mit einer Chipkarte erfolgen, während eine Ortung mittels GPS oder RFID stattfinden kann. Die Mensch-Roboter-Kollaboration erfordert regelmäßig nur, dass überhaupt die Anwesenheit eines Menschen oder die Ausrichtung seines Körpers erkannt werden.

Im Folgenden sollen dazu exemplarisch zwei Beispielszenarien untersucht werden:

- Zum einen die Erkennung eines Arbeitnehmers am Arbeitsplatz mittels Gesichtserkennung, um den Arbeitsplatz anhand der zu der jeweiligen Person hinterlegten Informationen individuell auf ihn einzustellen (Szenario 1).
- Zum anderen die Erfassung der Position sowie Körpergröße und -haltung eines Arbeitnehmers durch einen Roboter mittels optischer Sensoren oder Ultraschall, um Kollisionen zu vermeiden oder Werkstücke ergonomisch optimal anzureichen (Szenario 2).

3 Rechtliche Herausforderungen

Der Einsatz biometrischer Erkennung und sonstiger körperlicher Messungen in den genannten Szenarien wirft in erster Linie datenschutzrechtliche Fragestellungen auf. Dies meint vor allem die Frage, ob und wie der Arbeitgeber derartige Systeme einsetzen darf.

Datenschutz gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen (so bereits BVerfGE 65, 1, 43). Auf diese Weise soll das Persönlichkeitsrecht und die informationelle Selbstbestimmung betroffener Personen geschützt werden. Ist wegen der Verarbeitung personenbezogener Daten der Anwendungsbereich der DS-GVO eröffnet (3.1), bedarf es zur Rechtfertigung der Datenverarbeitung einer rechtlichen Erlaubnis (3.2). Biometrische Daten unterliegen dabei erhöhten Anforderungen, da von ihrer Verarbeitung besondere Risiken ausgehen. Überdies sind technische und organisatorische Vorkehrung (3.3) zur Verwirklichung eines effektiven Datenschutzes zu treffen.

3.1 Anwendungsbereich der DS-GVO

Die Anwendbarkeit des Datenschutzrechts setzt gem. Art. 2 Abs. 1 die (teil-)automatisierte oder dateimäßige Verarbeitung personenbezogener Daten voraus. Von einer automatisierten Datenverarbeitung ist im Kontext der Industrie 4.0 i.d.R. auszugehen. Es stellt sich damit die Frage nach der Verarbeitung personenbezogener Daten, d.h. von Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1).

Das Verständnis von Informationen i.S.v. Art. 4 Nr. 1 ist denkbar weit. Der Aussagegehalt, die Bedeutung oder die Art der Gewinnung der Informationen ist nicht entscheidend. Auch vermeintlich belanglose Daten werden erfasst (so bereits BVerfGE 65, 1, 45). Derartige Informationen sind bspw. Angaben zum Aussehen einer Person (z.B. Gesicht), zu körperlichen Maßen (z.B. Körpergröße, Armlänge), zur Körperhaltung (z.B. gebückt) oder zum Aufenthaltsort.

Die Informationen müssen sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dieser Bezug kann sich aus den Informationen selbst (z.B. Name und Anschrift) oder aus der Verknüpfung mit weiteren Informationen ergeben. Es ist darauf abzustellen, ob der für die Datenverarbeitung Verantwortliche (d.h. der Arbeitgeber) diesen Bezug, ggfs. unter Zuhilfenahme von (rechtmäßig) verfügbarem Zusatzwissen (z.B. dem Schichtplan), herstellen kann.

Die in Szenario 2 durch den Roboter, z.B. mittels optischer Sensoren, erfassten und verarbeiteten Informationen zu Position sowie Körpergröße und -haltung des Arbeitnehmers sind aus sich heraus nicht personenbezogen (z.B. Körpergröße 1.8 m oder Entfernung 2 m). Können sie aufgrund zusätzlicher Informationen einer Person zugeordnet werden, liegt hingegen Personenbezug vor (z.B. Arbeitnehmer X ist 1.8 m groß und befindet sich in 2 m Entfernung zur Maschine). Eine solche Zuordnung ist insbesondere möglich, wenn die Angaben durch den Roboter protokolliert werden (z.B. der jeweilige Abstand) und – etwa wegen vorheriger Anmeldung an der Maschine, aus dem Schichtplan oder durch Befragung von Kollegen – nachvollziehbar ist, wer zu einem bestimmten Zeitpunkt an der Maschine gearbeitet hat. Auch die Überschaubarkeit des Kollegenkreises ermöglicht eine Identifikation, wenn bestimmte körperliche Merkmale nur einmal in dem Betrieb vorkommen (z.B. eine bestimmte Größe, Armlänge, etc.).

Werden hingegen die Angaben zu Position sowie Körpergröße und -haltung von dem Roboter erfasst, unmittelbar verwertet und, nachdem der Roboter die erforderliche Handlung durchgeführt hat (z.B. die Haltung des Werkstückes korrigiert), sofort wieder rückstandsfrei gelöscht, ohne dass von außen eine irgendwie geartete Zugriffsmöglichkeit besteht, lässt sich vertreten, dass kein Personenbezug vorliegt. Es liegt keine Gefährdung der Persönlichkeitsrechte der jeweiligen Arbeitnehmer vor (vgl. hierzu BVerfGE 120, 378, 399). Eine spätere Zuordnung ist aufgrund der Löschung nicht möglich. Die technische Ausgestaltung der Maschine kann dementsprechend helfen, einen Personenbezug zu vermeiden oder zumindest die damit einherge-

hende Beeinträchtigung zu verringern. Eine andere Frage ist allerdings, ob eine solche Vorgehensweise gangbar ist, da zur Aufklärung von Unfällen sowie zur Klärung von Haftungsfragen eine Protokollierung der wesentlichen Funktionen einer Maschine erforderlich sein kann (z.B. Protokollierung einer Kollision oder Abstandsunterschreitung).

Findet – wie in Szenario 1 – eine biometrische Gesichtserkennung statt, liegen grundsätzlich personenbezogene Daten vor (zum Personenbezug biometrischer Daten [Horn04]). Dies betrifft regelmäßig alle Verfahrensschritte, jedenfalls wenn der Vorgang unter Kontrolle des Arbeitgebers stattfindet. Zunächst sind die verwendeten Abbildungen des menschlichen Gesichts i.d.R. personenbezogen, da hieraus auf das Aussehen einer bestimmten Person geschlossen werden kann. Während des Enrolements, d.h. der Erstellung und Speicherung eines Referenzdatensatzes durch Extraktion der biometrischen Merkmale (z.B. bestimmter Gesichtsmerkmale), ist ebenfalls von einem Personenbezug auszugehen. Personenbezug liegt auch vor, wenn die Referenzdaten mit einer Zuordnungsliste versehen (z.B. Name oder ID eines Arbeitnehmers) in einer Datenbank gespeichert werden. Werden für den Vergleich erneut biometrische Merkmale beim Arbeitnehmer erhoben und mit dem Referenzdatensatz abgeglichen, werden sowohl die Vergleichsdaten als auch die herangezogenen Referenzdaten regelmäßig personenbezogen sein.

Der Personenbezug der gespeicherten Referenzdaten (bzw. Referenztemplates) kann aufgehoben werden, wenn eine Speicherung ohne Zuordnungsliste (z.B. Name oder ID) erfolgt und keine Möglichkeit besteht, von den Referenzdaten auf die ursprünglichen Rohdaten (z.B. das Gesicht) zurückzurechnen. Dies gilt insbesondere bei Verwendung sog. geschützter Templates (z.B. ein aus den biometrischen Merkmalen errechnetes Chiffrat). Gerade bei großen Datenbanken kann es dann nicht mehr bestimmbar sein, welche Referenzdaten zu welcher Person gehören. Bei Vergleich der so gespeicherten Referenzdaten mit einem neu erhobenen Vergleichsdatensatz und Feststellung einer Übereinstimmung, sind die Referenzdaten allerdings wiederum personenbezogen, wenn die Vergleichsdaten (z.B. das Gesicht bzw. die daraus extrahierten Merkmale eines Arbeitnehmers) personenbezogen sind [Horn04].

Eine Möglichkeit, bei der biometrischen Erkennung den Personenbezug für den Arbeitgeber weitestgehend zu vermeiden, besteht darin, den Erkennungsvorgang auf ein Gerät zu verlagern, zu dem nur der Arbeitnehmer Zugriff hat. Z.B. kann ein Smartphone des Arbeitnehmers zur Erfassung des Gesichts genutzt werden, um dieses mit den auf dem Smartphone gespeicherten Referenzdaten abzugleichen. Bei Übereinstimmung wird lediglich das Ergebnis, z.B. Zugang ja / nein oder spezifische Einstellungsparameter, weitergeleitet.

Insgesamt wird im Kontext der Industrie 4.0 aufgrund vielfältiger Sensorik und digitaler Datenverarbeitung häufig ein Personenbezug vorliegen. Auch vordergründig maschinenbezogene Daten können personenbezogen sein, selbst wenn dies gar nicht beabsichtigt ist [HoHo17b].

3.2 Rechtliche Erlaubnis

Liegen personenbezogene Daten vor, ist für die Verarbeitung eine rechtliche Erlaubnis erforderlich (sog. Verbotsprinzip). Grundsätzlich gilt Art. 6 Abs. 1. Werden biometrische Daten verarbeitet, gelten die deutlich restriktiveren Erlaubnistatbestände des Art. 9 Abs. 2. Begründet wird dies in Erwägungsgrund (EwG) 51 mit den „erhebliche[n] Risiken für die Grundrechte und Grundfreiheiten“ bei der Verarbeitung biometrischer Daten. Im Beschäftigungsverhältnis ist überdies der zur Ausfüllung der Öffnungsklausel in Art. 88 erlassene § 26 BDSG zu berücksichtigen.

3.2.1 Biometrische Daten

Fraglich ist, ob Gesichtsaufnahmen sowie Informationen zu den Maßen der Gliedmaßen oder zur Position eines Körpers biometrische Daten i.S.d. DS-GVO sind. Die juristische Definition von Biometrie stimmt dabei nicht zwingend mit dem technischen Verständnis überein. Gem. Art. 4 Nr. 14 erfordert dies „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung […] ermöglichen oder bestätigen". Beispielhaft werden „Gesichtsbilder" sowie „daktyloskopische Daten" genannt.

Zunächst müssen „Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen" einer Person vorliegen. Physische und physiologische Merkmale beziehen sich auf den Körper und die damit verbundenen physikalischen, chemischen und biochemischen Lebensvorgänge. Dies umfasst auch Angaben zur Ausgestaltung des Gesichts (z.B. Gesichtstopographie) und zu Maßen der Gliedmaßen. Zum anderen werden verhaltenstypische Merkmale erfasst. Aus dem allgemeinen Begriffsverständnis von Biometrie (Messung am Lebewesen) sowie einem Vergleich mit den anderen Merkmalskategorien ergibt sich, dass diese Merkmale auf den Körper eines Menschen bezogen sein müssen. Angaben zum Sozialverhalten (z.B. Arbeitnehmer X holt sich immer um 09.35 Uhr einen Kaffee) werden nicht erfasst, die Dynamik des menschlichen Gangs oder das Tippverhalten hingegen schon. Dementsprechend ist auch die Angabe, dass Arbeitnehmer X in zwei Meter Entfernung zu einer Maschine steht, kein verhaltenstypisches Merkmal i.S.v. Art. 4 Nr. 14.

Die Daten zu diesen Merkmalen müssen personenbezogen sein, d.h. die Informationen müssen sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Biometrische Daten sind mithin ein Unterfall personenbezogener Daten.

Des Weiteren müssen sie eine „eindeutige Identifizierung" der Person „ermöglichen oder bestätigen". Da biometrische Erkennung aus technischer Sicht auf dem Vergleich, d.h. der Berechnung oder Messung der Ähnlichkeit zweier oder mehrerer Merkmalssätze beruht (biometrische Probe und biometrische Referenz), ist als „eindeutige Identifizierung" i.S.v. Art. 4 Nr. 14 die eindeutige Feststellung zu verstehen, dass die verglichenen Merkmalssätze von derselben Person stammen. Die Formulierung „ermöglichen oder bestätigen" kann als Hinweis auf die biometrische Identifikation (1:n) und Verifikation (1:1) verstanden werden.

Für eine eindeutige Identifizierung muss es sich bei den herangezogenen Merkmalen um hochcharakteristische Merkmale handeln. Diese müssen zwar nicht zwingend bei jedem Menschen weltweit einzigartig sein, sie müssen aber grundsätzlich geeignet sein, eine unbestimmte Zahl von Menschen eindeutig voneinander zu unterscheiden und dafür auch eine gewisse zeitliche Stabilität aufweisen [Weic18b].

Anerkannt ist dies z.B. bei spezifischen Ausprägungen der Papillarleisten (sog. Minutien), spezifischen Gesichtsmerkmalen oder auch dem Gang- oder Tippverhalten. Hingegen ermöglichen einzelne Angaben zu vielfach auftretenden Merkmalsausprägungen, etwa zur Nasenform (z.B. nubische Nase), Haarfarbe (z.B. blond) oder Schuhgröße (z.B. 42), keine eindeutige Identifizierung. Auch wird das Maß eines einzelnen Armes hierfür wohl nicht genügen. Dass derartige Merkmale bei sehr kleinen Personengruppen zur Identifizierung ausreichen (zwei Arbeitnehmer: einer rothaarig, einer blond), macht sie nicht zu biometrischen Daten i.S.v. Art. 4 Nr. 14, da das Vorliegen biometrischer Daten ansonsten von der jeweiligen Gruppengröße abhängig wäre und bei deren Veränderung (z.B. eine weitere rothaarige Person kommt hinzu) biometrische Daten plötzlich zu nicht-biometrischen Daten – oder umgekehrt –werden könnten. Dies

würde angesichts der unterschiedlichen Verarbeitungsvoraussetzungen in Art. 6 und Art. 9 eine massive Rechtsunsicherheit nach sich ziehen und ist nicht Zweck der Regelung in Art. 4 Nr. 14. Eine Kombination derartiger Merkmale (z.B. die Maße verschiedener Körperteile) kann wiederum derart spezifisch sein, dass auch bei einer sehr großen Personengruppe eine eindeutige Identifizierung möglich wird [Weic18b].

Dass die eindeutige Identifizierung aufgrund von Mess- oder Bedienfehlern im Einzelfall scheitern kann, ist unschädlich, solange die herangezogenen Merkmale grundsätzlich eine eindeutige Identifizierung ermöglichen. Eine hundertprozentige Genauigkeit bei der Identifizierung ist technisch nicht möglich. Es kann daher nicht angenommen werden, dass der Gesetzgeber sie als Definitionsmerkmal regeln wollte.

Die Daten zu den spezifischen Merkmalen einer Person müssen mit „speziellen technischen Verfahren“ gewonnen worden sein. EwG 51 S. 3 bestimmt, dass Lichtbilder nur als biometrische Daten anzusehen sind, wenn „sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung […] ermöglichen“. Technische Verfahren zur Anfertigung von Lichtbild- und Videoaufnahmen oder – allgemeiner gesprochen – zur (digitalen) Abbildung des menschlichen Körpers oder Verhaltens sind somit noch keine „speziellen technischen Verfahren“ i.S.v. Art. 4 Nr. 14. Vielmehr müssen aus diesen Abbildungen des menschlichen Körpers oder Verhaltens spezifische physische, physiologische oder verhaltenstypische Merkmale abgeleitet (d.h. extrahiert) werden, die dann eine eindeutige Erkennung ermöglichen. So sind bloße Abbildungen eines menschlichen Gesichts oder Daumens (z.B. durch eine Kamera erfasst) noch keine biometrischen Daten, die aus der Darstellung des Gesichts extrahierten spezifischen Merkmale bzw. aus der Papillarleistenstruktur des Daumens extrahierten Minutien hingegen schon. Es sind also diese hochcharakteristischen Merkmalsinformationen, durch Extraktion gewonnen und ggfs. als Referenzdatensatz (Referenztemplate) gespeichert, die die Definition biometrischer Daten i.S.v. Art. 4 Nr. 14 erfüllen; s.a. [Jand18].

Fraglich ist, ob die „speziellen technische Verfahren“ automatisiert bzw. teilautomatisiert ablaufen müssen, oder ob auch ein rein händisches Vorgehen (z.B. ein anthropologisches Sachverständigengutachten zum Gesichtsvergleich) erfasst wird. Der Anwendungsbereich der DS-GVO ist gem. Art. 2 Abs. 1 auch bei der nichtautomatisierten Verarbeitung eröffnet, wenn die Daten in einem Dateisystem, d.h. einer strukturierten Sammlung (Art. 4 Nr. 6), gespeichert werden. Mit Blick darauf, dass Art. 4 Nr. 14 (i.V.m. Art. 9) das erhöhte Risiko für die Grundrechte und Grundfreiheiten bei Verarbeitung biometrischer Daten wiederspiegelt (EwG 51 S. 1), ist davon auszugehen, dass nur (teil-)automatisierte Verfahren erfasst sind; v.a. hinsichtlich der Extrahierung und des Vergleichs der Merkmale. Händischen Verfahren kommt aufgrund ihrer Langsamkeit und ihrer nicht-digitalen Form keine besondere Eignung zur Überwachung oder Erstellung von Persönlichkeitsprofilen zu. Damit verbundene Risiken bedürfen keiner spezifischen Regulierung. Überdies spricht auch das allg. Wortlautverständnis von Biometrie bzw. biometrischer Erkennung (s.o.) für ein (teil-)automatisiertes Verfahren.

Bezogen auf die Szenarien bedeutet dies, dass bloße Gesichtsbilder keine biometrischen Daten sind. Daraus extrahierte spezifische Merkmale, die als Template gespeichert und für eine biometrische Erkennung genutzt werden können, unterfallen hingegen dem Begriff der biometrischen Daten (Szenario 1). Informationen zum Abstand eines Arbeitnehmers zu einer Maschine oder zur Position im Raum sind wiederum keine biometrischen Daten. Dies gilt auch für die Vermessung der Körperhöhe oder einzelner Gliedmaßen (Szenario 2).

3.2.2 Einzelne Erlaubnistatbestände

Zentrale Erlaubnisregelung für die Datenverarbeitung im Beschäftigungsverhältnis ist § 26 BDSG. Die erforderliche Erlaubnis kann sich v.a. aus einer Einwilligung, einer Betriebsvereinbarung oder aus dem Zweck des Beschäftigungsverhältnisses ergeben. In letztgenanntem Fall findet sich die Unterscheidung bei der Erlaubnis der Verarbeitung „normaler“ (Art. 6) und biometrischer Daten (Art. 9) in § 26 Abs. 1 u. 3 BDSG wieder. Für eine gewisse Rechtsunsicherheit sorgt der Umstand, dass die Europarechtskonformität des § 26 BDSG teilweise bestritten wird [Masc18a] [Masc18b]. Nichtsdestotrotz ist er derzeit geltendes Recht.

Einwilligung

Sowohl Art. 6 Abs. 1 lit. a als auch Art. 9 Abs. 2 lit. a sehen als Erlaubnis die Einwilligung (Art. 4 Nr. 11) vor. Zu berücksichtigen sind die speziellen Vorgaben für Beschäftigungsverhältnisse gem. § 26 Abs. 2 u. 3 Satz 2 BDSG.

Im Rahmen der Einwilligung ist insbesondere das Erfordernis der Freiwilligkeit problematisch (s. § 26 Abs. 2 BDSG). Die strukturelle Unterlegenheit des Arbeitnehmers gegenüber dem Arbeitgeber kann zu Drucksituationen führen, die die Freiwilligkeit – und damit eine rechtmäßige Einwilligung – ausschließen. Verweigern einzelne Arbeiter die Einwilligung, muss der Arbeitgeber ggfs. Alternativen anbieten, die nicht mit der Verarbeitung derartiger Daten einhergehen. Während dies bspw. bei der Zugangssicherung am Eingangstor durch Rückgriff auf Sicherheitspersonal noch handhabbar erscheint, ist dies z.B. im Bereich der Mensch-Roboter-Kommunikation kein gangbarer Weg. Die Einwilligung ist in den hier interessierenden Konstellationen i.d.R. keine geeignete Verarbeitungsgrundlage [Hofm16] [HoSt05].

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

§ 26 Abs. 1 BDSG regelt die Datenverarbeitung zur Durchführung eines Beschäftigungsverhältnisses. Der Rückgriff auf diesen Erlaubnistatbestand ist insbesondere von Interesse, wenn eine Betriebsvereinbarung (s.u.) in Ermangelung eines Betriebsrates ausfällt. Die Verarbeitung ist nur zulässig, wenn sie für Zwecke des Beschäftigungsverhältnisses erforderlich ist. Dies bedeutet im Ergebnis eine Abwägung zwischen den Interessen des Arbeitsgebers und dem Persönlichkeitsrecht der Beschäftigten (BT-Drs. 18/11325, S. 97). Es ist also der Grundsatz der Verhältnismäßigkeit zu wahren, d.h. es muss ein legitimer Zweck mit geeigneten, erforderlichen und angemessenen Mitteln verfolgt werden [Masc18a]. Zur Wahrung der Grundprinzipien des Datenschutzes (Art. 5) sind gem. § 26 Abs. 5 BDSG geeignete technische und organisatorische Maßnahmen (s. Art. 25 u. 32) zu treffen.

Werden personenbezogene Daten der Arbeitnehmer zur Abstandsmessung oder der ergonomischen Anreichung von Werkstücken im Rahmen der Mensch-Roboter-Kollaboration verarbeitet (Szenario 2), dient dies der Durchführung eines Beschäftigungsverhältnisses, da die Verarbeitung im Zusammenhang steht mit der Pflicht des Arbeitnehmers zur Erbringung der geschuldeten Arbeitsleistung an der Maschine sowie der Pflicht des Arbeitgebers, einen sicheren Arbeitsplatz zur Verfügung zu stellen.

Die konkret verfolgten Zwecke der Unfallverhütung sowie der ergonomischen Anreichung sind legitim und die Datenverarbeitung zur Erreichung auch geeignet. Dies gilt auch für ggfs. stattfindende Protokollierungen zur Unfallermittlung oder zu Wartungszwecken. Gleich wirksame, aber milder wirkende Mittel sind nicht ersichtlich. Insbesondere ist eine Zweckerreichung ohne Verarbeitung personenbezogener Daten i.d.R. nicht möglich. Es ist auch nicht ersichtlich, dass Arbeitnehmer durch diese Form der Datenverarbeitung unangemessen benachteiligt werden.

Die Datenverarbeitung betrifft keine Informationen, die der Privat- oder Intimsphäre zuzuordnen sind. Sie ist überdies z.T. auch im offensichtlichen Interesse der Arbeitnehmer (Kollisionsvermeidung, ergonomisches Anreichen). Ein unberechtigter oder für die genannten Zwecke nicht erforderlicher Zugriff auf die Daten kann durch ein Rechte- und Rollenkonzept verhindert werden (Art. 32). In diesem Zusammenhang sollte auch festgelegt werden, dass die Daten nicht für eine den Arbeitnehmer ungleich stärker belastende Leistungsüberwachung genutzt werden dürfen.

§ 26 Abs. 3 BDSG regelt die Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1, was auch biometrische Daten umfasst. Eine Verarbeitung für Zwecke des Beschäftigungsverhältnisses ist zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Die in § 26 Abs. 3 BDSG vorgesehene Interessenabwägung ist somit strenger („kein Grund zu der Annahme“) als die in § 26 Abs. 1 BDSG.

Wird biometrische Erkennung zur Individualisierung des Arbeitsplatzes eingesetzt (Szenario 1), dient dies der Erfüllung individualvertraglicher Rechte und Pflichten aus dem Arbeitsrecht. Wie auch bei § 26 Abs. 1 BDSG ist eine Verhältnismäßigkeitsprüfung durchzuführen, wobei bereits die Annahme, dass schutzwürdige Interessen der betroffenen Person (d.h. Arbeitnehmer) überwiegen, die Datenverarbeitung unzulässig macht.

Die Verarbeitung biometrischer Daten zur individuellen Einstellung des Arbeitsplatzes verfolgt einen legitimen Zweck und ist zur Zweckerreichung auch geeignet. Zwar ist eine Individualisierung auch durch den Einsatz einer Chipkarte, die Eingabe einer Benutzerkennung oder einen am Körper getragenen RFID-Transponder möglich. Dies kostet aber i.d.R. mehr Zeit als ein Blick in eine Kamera, was insbesondere bei ständig wechselnden Arbeitsplätzen bedeutsam ist (z.B. im Logistikbereich), bzw. bietet nicht das gleiche Maß an Sicherheit, da Chipkarten, Benutzerkennungen und RFID-Transponder weitergegeben werden können. Im Rahmen der Angemessenheitsprüfung ist zu berücksichtigen, dass die Verarbeitung biometrischer Daten i.S.v. Art. 4 Nr. 14 schwerer wiegt als die Verarbeitung körperbezogener Daten in Szenario 1. Wegen der (z.T. lebenslangen) Bindung biometrischer Daten an eine bestimmte Person sowie ihre Eignung zur Überwachung und Profilbildung kommt der Gewährleistung von Datensicherheit große Bedeutung zu. Aufgrund des Verweises in § 26 Abs. 3 S. 3 BDSG auf § 22 Abs. 2 BDSG wird die Notwendigkeit unterstrichen „angemessene und spezifische Maßnahmen“ vorzusehen, welche die Interessen der Person, deren sensible Daten verarbeitet werden, wahren soll [Masc18a]. Dies betrifft z.B. Maßnahmen zur Verschlüsselung hinterlegter Referenzdaten und ein Rechte- und Rollenkonzept bzgl. des Zugriffs auf die Daten. Im Ergebnis kommt es damit auf den Einzelfall an.

Betriebsvereinbarung

Mit § 26 Abs. 4 S. 1 BDSG hat der deutsche Gesetzgeber klargestellt, dass die Verarbeitung von personenbezogenen Daten – einschließlich biometrischer Daten (als besondere Kategorie personenbezogener Daten i.S.v. Art. 9 Abs. 1) – von Beschäftigten für Zwecke des Beschäftigungsverhältnisses zulässig ist. Erforderlich dazu ist eine Befugnis im Rahmen einer Kollektivvereinbarung (vgl. bereits Art. 88 Abs. 1). Kollektivvereinbarungen sind Tarifverträge und Betriebsvereinbarungen. Auch außerhalb des Anwendungsbereichs des Datenschutzrechts ist eine Betriebsvereinbarung gem. § 87 Abs. 1 Nr. 6 BetrVG erforderlich, wenn es um die Ein-

führung und Anwendung von technischen Einrichtungen geht, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Dementsprechend hat § 26 Abs. 4 BDSG in Bezug auf die DS-GVO im Ergebnis nur eine klarstellende Funktion [Masc18a].

Entscheidend ist, dass die Verarbeitung der Daten erforderlich ist, geeignete Garantien zum Schutz der Grundrechte bestehen und die Interessen des Betroffenen gewahrt werden [Masc18a]. Die Betriebsvereinbarung (§ 77 BetrVG) kann den dazu erforderlichen eigenständigen Erlaubnistatbestand darstellen, der unmittelbar und zwingend wirkt (§ 77 Abs. 4 BetrVG) [Ries18a] [Weic18a]. Der Gang über eine Betriebsvereinbarung ist oftmals vorzugswürdig [Alb07]. Ermöglicht wird den Verhandlungsparteien so nämlich eine auf die betrieblichen Bedürfnisse zugeschnittene Ausgestaltung, die einerseits flexibel und maßgeschneidert, anderseits für alle verbindliche ist. Dabei bietet sich an, unbestimmte Rechtsbegriffe zu präzisieren und Regelungen der Modalitäten zum konzernweiten Datenfluss zu treffen [Masc18a].

Im Rahmen der Betriebsvereinbarung sind die Parteien an die Grundsätze des Art. 88 Abs. 2 gebunden (§ 26 Abs. 4 S. 2 BDSG). Dies bedeutet, dass geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, getroffen werden müssen. Darüber hinaus sind die allgemeinen Grundsätze gem. Art. 5 zu beachten.

Eine Absenkung des Datenschutzes unter das Niveau der DS-GVO ist unzulässig [Ries18b] [Masc18a] [ScSo14]. Vielmehr setzt die DS-GVO einen Mindeststandard fest, der durch die Betriebsvereinbarung präzisiert und konkretisiert werden kann.

Die Betriebsvereinbarung unterliegt einer Verhältnismäßigkeitskontrolle und findet ihre Grenzen in der Wahrung der Persönlichkeitsrechte der Arbeitnehmer (§ 75 Abs. 2 BetrVG). Die grundsätzlichen Wertungen des Datenschutzrechts müssen dabei Berücksichtigung finden. Im Endeffekt läuft dies auf eine Güterabwägung zwischen den Interessen des Arbeitgebers und den Persönlichkeitsrechten und berechtigen Interessen der Arbeitnehmer hinaus. Zu berücksichtigen sind dabei die jeweiligen Umstände des Einzelfalls [Masc18b]. Bei gleich wirksamen, aber weniger einschränkenden Mitteln ist der Einsatz auf diese zu beschränken. Im Ergebnis darf die Schwere des Eingriffes nicht außer Verhältnis zum verfolgten Zweck stehen [Masc18a]. Im Kontext der Biometrie ist somit insbesondere zu untersuchen, inwieweit es alternative Möglichkeiten gibt, die die Arbeitsläufe genauso vereinfachen. Des Weiteren sind die Interessen des Arbeitnehmers in ausreichendem Maße durch technische und organisatorische Maßnahmen zu schützen.

Überdies ist die Mitbestimmung des Betriebsrates zu beachten (§ 87 Abs. 1 Nr. 6 BetrVG; zur Mitbestimmungspflichtigkeit biometrischer Zugangssicherungssysteme BAGE 109, 235). Gem. § 26 Abs. 7 BDSG gilt das Gesagte auch für solche Daten, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

3.2.3 Verbot automatisierter Einzelentscheidung

Art. 22 Abs. 1 verbietet Entscheidungen, die ausschließlich auf einer automatisierten Datenverarbeitung beruhen und gegenüber dem Betroffenen eine rechtliche Wirkung oder eine ähnliche erhebliche Beeinträchtigung entfalten. Fraglich ist, ob die Entscheidung über die Individualisierung des Arbeitsplatzes (Szenario 1) und über das Abstandhalten sowie das ergonomische Anreichen von Werkstücken (Szenario 2) hiervon erfasst wird.

Die Vorgängerregelungen in § 6a BDSG a.F. bzw. Art. 15 DSRL 95/46/EG forderten die „Bewertung einzelner Persönlichkeitsmerkmale“ bzw. „einzelner Aspekte ihrer Person“. Eine solche Bewertung der Person liegt bei der biometrischen Erkennung und sonstigen körperlichen Messungen i.d.R. nicht vor, da sie nur zur Erkennung des Merkmalsträgers benutzt werden [Scho14], so dass das Verbot der automatisierten Einzelentscheidung bereits aus diesem Grund nicht einschlägig war. Art. 22 sieht eine derartige Bewertung nicht mehr vor. Dem Wortlaut nach wird daher jede Entscheidung erfasst, die ausschließlich auf einer automatisierten Verarbeitung beruht. In der Literatur wird z.T. unter Hinweis auf EwG 71 S. 1 („persönlichen Aspekten“) gefordert, das Erfordernis der Bewertung einzelner Persönlichkeitsmerkmale in Art. 22 hineinzulesen [Buch17], so dass biometrische Erkennung sowie sonstige körperliche Messungen bereits aus diesem Grund in den genannten Szenarien nicht erfasst wären.

Jedenfalls aber entfaltet die Entscheidung in den genannten Szenarien keine rechtliche Wirkung i.S.v. Art. 22 gegenüber betroffenen Arbeitnehmern, da ihre Rechtspositionen durch die Identifizierung nicht verändert werden (anders z.B. bei Kündigung oder Beförderung). Auch werden sie nicht in ähnlicher Weise erheblich beeinträchtigt, insbesondere werden sie weder in ihrer wirtschaftlichen noch ihrer persönlichen Entfaltung nachhaltig gestört; s. dazu [Buch17].

3.3 Technische und organisatorische Maßnahmen

Bei Verarbeitung personenbezogener Daten bedarf es nicht nur einer gesetzlichen Erlaubnis (Art. 5 Abs. 1 lit. a: „Rechtmäßigkeit“, s. 3.2). Es sind darüber hinaus auch technische und organisatorische Maßnahmen zu treffen, um die Beachtung der Grundsätze des Art. 5 Abs. 1 zu gewährleisten. Erforderlich ist eine für den Betroffenen nachvollziehbare Verarbeitung („Transparenz“). Außerdem ist sicherzustellen, dass Daten nur für festgelegte legitime Zwecke verarbeitet werden („Zweckbindung“) und die Verarbeitung nicht über das Erforderliche Maß hinausgeht („Datenminimierung“ und „Speicherbegrenzung“). Es muss überdies ein angemessener Schutz vor unbefugten Zugriffen bestehen („Integrität und Vertraulichkeit“).

Gem. Art. 5 Abs. 2 muss der Verantwortliche die Einhaltung der Grundsätze nachweisen können („Rechenschaftspflicht”). Das erfordert die Festlegung interner Strategien (EwG 78 Satz 2) sowie die Ergreifung technischer und organisatorischer Maßnahmen zur Gewährleistung von Datenschutz durch Technikgestaltung (Art. 25) und Datensicherheit (Art. 32). Dahinter steht der Gedanke, dass Datenschutz nicht nur rechtlich sondern auch technisch zu gewährleisten ist.

Im Einzelnen sollte soweit wie möglich auf die Verarbeitung personenbezogener Daten verzichtet werden. Dies erscheint im Bereich der datenintensiven Industrie 4.0 aber nur schwer möglich. Für den Bereich biometrischer Erkennung ist bspw. an den Verzicht der Verknüpfung hinterlegter Referenzdaten mit den Klarnamen der Betroffenen sowie anonymisiertes Referenzmaterial zu denken [Däub17]. Auch bietet es sich an, die Verarbeitung biometrischer Daten nach Möglichkeit in die Sphäre des Arbeitnehmers zu verlagern [GoPW16].

Ein Rechte- und Rollenkonzept sollte den Zugriff auf die Daten regeln. Dies umfasst ein System abgestufter Zugriffsrechte, um zu verhindern, dass unberechtigt Daten abgerufen werden. Bei Daten, die Aufschluss über die Leistung geben, ist eine Abgrenzung zur Personalabteilung zu empfehlen. Die Protokollierung der Datenzugriffe sorgt für Nachvollziehbarkeit. Gerade bei biometrischen Systemen ist ein hohes Maß an Datensicherheit notwendig (zur Sicherheit biometrischer Systeme [JaRN11] [Adle08]).

Betriebliche Datenschutzbeauftragte (Art. 37 ff., § 38 BDSG) sind frühzeitig einzubinden. Eine Abstimmung mit der zuständigen Aufsichtsbehörde ist anzuraten (Art. 51 ff.). Die DS-GVO

erfordert überdies das Führen eines Verfahrensverzeichnisses (Art. 30) sowie – bei besonders gefahrgeneigten Verarbeitungen – die Durchführung einer Datenschutz-Folgenabschätzung (Art. 35). Schließlich können Löschroutinen sicherstellen, dass nicht benötigte Daten nicht unnötig vorgehalten werden. Zu berücksichtigen ist dabei allerdings, dass ggfs. gesetzliche Verpflichtungen ein weiteres Vorhalten der Daten verlangen können.

4 Fazit & Ausblick

Der Einsatz von Biometrie im Bereich Industrie 4.0 ist weder nach der neuen DS-GVO noch nach den Änderungen im deutschen Datenschutzrecht von vornherein ausgeschlossen. Die Zulässigkeit des Einsatzes von biometrischen Daten ist im Einzelfall zu entscheiden.

Empfehlenswert ist der Abschluss einer Betriebsvereinbarung, die die Interessen des Arbeitnehmers und des Arbeitgebers in einen angemessenen Ausgleich zueinander bringt. Dabei kommt es insbesondere auf den vorher festgelegten Zweck an. Zur Absicherung sind geeignete technische und organisatorische Maßnahmen zu treffen, die das besondere Risiko biometrischer Daten minimieren. Insbesondere die technische Gestaltung dient maßgeblich zur Einhaltung der Datenschutzgrundsätze.

Eine Auseinandersetzung mit den erforderlichen Voraussetzungen ist nicht zuletzt aufgrund der drastisch erhöhten Bußgelder bei Verstößen (bis zu 20 Mio. Euro bzw. vier Prozent des weltweiten Jahresumsatzes, Art. 83) erforderlich. Die Rechtsunsicherheit, z.B. durch den vom deutschen Gesetzgeber geschaffenen § 26 BDSG sowie die fehlende Rechtsprechung des EuGH zur neuen Rechtslage, tut ihr Übriges. Eine Orientierung und Berücksichtigung der Interessen des Arbeitnehmers in ausreichendem Maße minimiert das Risiko dennoch erheblich, so dass auch Biometrie auf dem betrieblichen Hallenboden erfolgreich eingeführt werden kann.

Literatur

[Adle08] A. Adler: Biometric System Security. In: A. Jain, P. Flynn, A. Ross (Hrsg,): Handbook of Biometrics, Springer (2008) 381-402.

[Alb07] A. Albrecht: Biometrie am Arbeitsplatz — Konkrete Ausgestaltung der Mitbestimmung. In: Datenschutz und Datensicherheit (DuD) (2007) 171-175.

[BBB+08] H. Biermann, M. Bromba, C. Busch, G. Hornung, M. Meints, G. Quiring-Kock: White Paper zum Datenschutz in der Biometrie, TELETRUST Deutschland e.V. (2008).

[Buch17] B. Buchner: Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling. In: J. Kühling, B. Buchner (Hrsg): Datenschutz-Grundverordnung Kommentar, C.H.Beck (2017), 471-481.

[Däub17] W. Däubler: Gläserne Belegschaft. Das Handbuch zum Beschäftigtendatenschutz, BUND Verlag (2017).

[GoPW16] P. Gola, S. Pötters, G. Wronka: Handbuch Arbeitnehmerdatenschutz unter Berücksichtigung der Datenschutz-Grundverordnung, DataKontext (2016).

[Hofm16] K. Hofmann: Smart Factory - Arbeitnehmerdatenschutz in der Industrie 4.0 - Datenschutzrechtliche Besonderheiten und Herausforderungen. In: Zeitschrift für Datenschutz (ZD) (2016) 12-17.

[Horn04] G. Hornung: Der Personenbezug biometrischer Daten. In: Datenschutz und Datensicherheit (DuD) (2004) 429-431.

[HoHo17a] G. Hornung, K. Hofmann: Industrie 4.0 und das Recht: Drei zentrale Herausforderungen, acatech – Deutsche Akademie der Technikwissenschaften (2017).

[HoHo17b] G. Hornung, K. Hofmann: Rechtsfragen bei Industrie 4.0: Rahmenbedingungen Herausforderungen und Lösungsansätze. In: G. Reinhart (Hrsg.): Handbuch Industrie 4.0, Hanser (2017) 191-212.

[HoSt05] G. Hornung, R. Steidle: Biometrie am Arbeitsplatz – sichere Kontrollverfahren versus ausuferndes Kontrollpotential. In: Arbeit und Recht (2005) 201-207.

[JaRN11] A. Jain, A. Ross, K. Nandakumar: Introduction to Biometrics, Springer (2011).

[Jand18] S. Jandt: Biometrische Videoüberwachung – was wäre wenn ... In: Zeitschrift für Rechtspolitik (ZRP) (2018) 16-19.

[Masc18a] F. Maschmann: § 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses. In: J. Kühling, B. Buchner (Hrsg.): Datenschutz-Grundverordnung Kommentar, C.H.Beck (2018), 1385-1420.

[Masc18b] F. Maschmann: Art. 88 Datenverarbeitung im Beschäftigungskontext.. In: J. Kühling, B. Buchner (Hrsg.): Datenschutz-Grundverordnung Kommentar, C.H.Beck (2018), 1177-1208.

[PrBj08] S. Prabhakar, V. Bjorn: Biometrics in the Commercial Sector. In: A. Jain, P. Flynn, A. Ross (Hrsg,): Handbook of Biometrics, Springer (2008) 479-507.

[ReZü17] G. Reinhart, D. Zühlke: Von CIM zu Industrie 4.0. In: G. Reinhart (Hrsg.): Handbuch Industrie 4.0, Hanser (2017) XXXI-XL.

[Ries18a] K. Riesenhuber: § 26 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses. In: S. Brink, H. Wolff (Hrsg.): BeckOK Datenschutzrecht, C.J.Beck (2018).

[Ries18b] K. Riesenhuber: Artikel 88 Datenverarbeitung im Beschäftigungskontext. In: S. Brink, H. Wolff (Hrsg.): BeckOK Datenschutzrecht, C.J.Beck (2018).

[Scho14] P. Scholz: § 6a Automatisierte Einzelentscheidung. In: S. Simitis (Hrsg.): Bundesdatenschutzgesetz, Nomos (2014) 696-715.

[ScSo14] P. Scholz, B. Sokol: § 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung. In: S. Simitis (Hrsg.): Bundesdatenschutzgesetz, Nomos (2014) 446-470.

[Weic18a] T. Weichert: Art. 9 Verarbeitung besonderer Kategorien personenbezogener Daten. In: J. Kühling, B. Buchner (Hrsg.): Datenschutz-Grundverordnung Kommentar, C.H.Beck (2018), 319-358.

[Weic18b] T. Weichert: Art. 4 Nr. 14 biometrische Daten. In: J. Kühling, B. Buchner (Hrsg.): Datenschutz-Grundverordnung Kommentar, C.H.Beck (2018), 186-188.