Herausragende Masterarbeiten

Autor*in

Michael Pelster

Studiengang

Wirtschaftsrecht für die Unternehmenspraxis, LL.M.

Masterarbeitstitel

Arbeitnehmerdatenschutz beim Einsatz vernetzter IoT-Sensorik in gewerblich genutzten Gebäuden

Distance and Independent Studies Center
DISC

Glossar

Begriff	Erläuterung
BLE	Bluetooth Low Energy Weiterentwicklung des Bluetooth-Standards, der mit geringen Energieverbräuchen auskommt und damit lange Batterielaufzeiten bei IoT-Geräten ohne feste Stromversorgung ermöglicht.
Bluetooth	Kurzstrecken-Funkprotokoll zur Übertragung aller Arten von Daten. Bei geringen Ansprüchen an die Bandbreite (typischerweise bei IoT-Anwendungen) sehr energieeffizient. Reichweite bis 100 m, in Gebäuden bis 15 m. Durch Aufbau eines Mesh-Netzwerkes können die Reichweiten erheblich vergrößert werden.
Firmware	Mikroprozessorbasierte Systeme besitzen in der Regel kein Betriebssystem. Die Firmware bestimmt ihre Programmlogik.
IIoT	Industrial Internet of Things Spezifizierung des IoT auf industriellen und gewerblichen Einsatz.
IoT	Internet of Things Allgemeine Bezeichnung für Technologien, die physische Dinge um Sensorik und/oder Aktorik erweitern, so dass sie mit anderen Dingen oder Systemen interagieren können.
LoRaWAN	Long Range Wide Area Network Übertragungsstandard im lizenzfreien Frequenzband 868 MHz, gedacht für kleine Datenmengen, jedoch mit hoher Reichweite auch innerhalb von Gebäuden und sehr geringem Stromverbrauch. Geeignet für batteriebetriebene Geräte.

LPWAN	Low Power Wide Area Network Sammelbegriff für Übertragungstechnologien, die mit geringem Energiebedarf hohe Reichweiten erzielen. Dies geht auf Kosten der Bandbreite, so dass nur geringe Datenmengen übertragen werden können, was jedoch bei den kleinen Paketen typischer IoT-Daten keine Rolle spielt. Beispiele für LPWAN-Protokolle sind SigFox und LoRaWAN.
Mesh-Netzwerk	Netzwerk, bei dem jeder Teilnehmer als Relaisstation für die Signale anderer Teilnehmer dient. Durch diese Verkettung lässt sich eine Reichweitenerhöhung gegenüber der direkten Punkt-zu-Punkt-Übertragung erzielen.
SigFox	Standard mit ähnlichen Funk-Eigenschaften wie LoRaWAN, jedoch betrieben von einem zentralen Netzbetreiber, dadurch keine Funktionsgarantie bei dessen Ausfall.
Unumkehrbare Kryptologische Hashfunktion	Verfahren, nach dem ein Ausgangswert in einen eindeutigen Zielwert umgerechnet wird. Aus dem Zielwert lässt sich der Ausgangswert nicht rekonstruieren. Als sicheres Verfahren gilt SHA-2 (Details s. https://de.wikipedia.org/wiki/SHA-2)
Zigbee	Kurzstrecken-Funkprotokoll zur Übertragung von Sensor- oder Aktordaten auf Strecken bis 100 m, in Gebäuden bis 15 m. Durch Aufbau eines Mesh-Netzwerkes können die Reichweiten erheblich vergrößert werden.

Inhaltsverzeichnis

Teil 1: Einleitung

A. Problemstellung

Der Beschäftigtendatenschutz ist in den vergangenen Jahrzehnten in seiner Bedeutung von einem Randthema zu einem allgegenwärtig präsenten Rechtsbereich herangewachsen.[1] Einer der Gründe hierfür ist die Digitalisierung der Arbeitswelt. So ist die weltweit erzeugte Datenmenge, zu der auch Daten in Unternehmensprozessen gehören, in den letzten 10 Jahren jährlich um 20 bis 30% angestiegen, Prognosen für die nächsten Jahre zeigen ein vergleichbares exponentielles Wachstum.[2]

An der Erhebung und Auswertung der Daten, die innerhalb ihrer Prozesse entstehen, haben Unternehmen ein wirtschaftliches Interesse. So konnte gezeigt werden, dass Unternehmen, die datengetrieben arbeiten, einen Wettbewerbsvorteil gegenüber Marktbegleitern erreichen, die ihr Datenpotenzial nicht ausschöpfen.[3] Wenn also unternehmensseitig ein natürliches Interesse an der Auswertung von Daten besteht, wächst gleichzeitig das Bedürfnis auf der Beschäftigtenseite an einer angemessenen Würdigung des Schutzes von Personendaten, die unweigerlich Teil des wachsenden Datenvolumens sind. Hier gibt es Bereiche mit besonderem Handlungsbedarf, zu deren Identifikation es nützlich ist, entstehende Personendaten in zwei Arten zu unterteilen:

Zum einen fallen, z.B. bei der Erfassung von Arbeitszeiten oder der Messung von Leistungen, Daten mit offensichtlichem Personenbezug an. Bei der Einführung solcher Geschäftsprozesse liegt auf der Hand, dass der Beschäftigtendatenschutz als fester Projektbestandteil angemessene Beachtung finden muss.

Zum anderen jedoch gibt es eine Vielzahl von Digitalisierungsfeldern im gewerblichen Umfeld, bei denen ein Personenbezug der anfallenden Daten auf den ersten Blick nicht in vollem Umfang erkennbar ist. Jedoch lassen sich durch die Kombination mit weiteren Datenquellen oder die Anwendung anderer analytischer Methoden oftmals mehr und sensiblere Daten mit Personenbezug ableiten als ursprünglich angenommen. Ein Beispiel hierfür sind Projekte aus dem Bereich „Industrial Internet of Things“ (IIoT). Diese Sparte der Digitalisierung hat in den

[1] *Düwell*, in: *Weth* et al., Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 2 ff.
[2] N.N., IDC - Volumen der jährlich generierten/replizierten digitalen Datenmenge weltweit von 2010 bis 2022 und Prognose bis 2027 (in Zettabyte) (https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/, abgerufen am 04.11.2023).
[3] *Ramadan/Shuqqo et al.*, Applied Sciences 2020, 6784.

letzten 5 Jahren ein konstantes Wachstum erfahren. Der Umsatz lag 2022 allein in Deutschland bei ca. 9 Milliarden Euro; ein Wachstum von jährlich rd. 13% wird prognostiziert.[4] Analog zu dieser Steigerung nimmt naturgemäß die Datenmenge mit potenziellem Personenbezug zu. Da diese Tatsache jedoch möglicherweise nicht erkannt wird oder zumindest nicht im Fokus der Prozessplanung steht, besteht die Gefahr, dass sie bei Planung, Umsetzung und Regelbetrieb solcher Projekte nicht angemessen berücksichtigt wird.

B. Zielsetzung

Die Arbeit soll anhand zweier Projektbeispiele aus dem Bereich der Digitalisierung gewerblich genutzter Gebäude, einem Teilbereich des IIoT, untersuchen, ob und in welchem Umfang beim geplanten Betrieb eines IIoT-Systems personenbezogene Daten als Nebenprodukt der eigentlich begehrten Nutzdaten und Funktionen entstehen können.

Im Weiteren soll eine Einordnung der im Planungsstand entstehenden datenschutzrechtlichen Situation anhand bestehender Gesetze und Verordnungen, entwickelter Rechtsprechung und der Diskussion in der Rechtswissenschaft vorgenommen werden.

Aus diesen Erkenntnissen werden organisatorische und technische Lösungen für die datenschutzrechtlichen Herausforderungen beider IIoT-Projekte aufgezeigt. Sie sollen dem wirtschaftlichen Interesse des Unternehmens ebenso gerecht werden wie dem Schutz der persönlichen Sphäre betroffener Beschäftigter.

Schließlich sollen Handlungsempfehlungen bei der Planung und Durchführung zukünftiger IIoT-Projekte für die Unternehmenspraxis abgeleitet werden.

[4] Marković, Industrielles IoT - Marktdaten-Analyse (https://de.statista.com/statistik/studie/id/146076/dokument/industrielles-iot-marktdaten-und-analyse/, abgerufen am 18.11.2023).

Teil 2: Hauptteil

A. Grundlagen

I. Technische Grundlagen: Erläuterungen und Stand der Entwicklung zu Smart Buildings

1. Das „Internet of Things“ (IoT)

Der Oberbegriff „IoT“ beschreibt die Ausstattung von Gegenständen mit technischen Komponenten, die Umgebungsdaten aufnehmen („Sensorik“) und ggf. auf die Umgebung einwirken können („Aktorik“). Gleichzeitig können solcherlei ausgestattete Gegenstände in aller Regel mit angebundenen Netzwerken kommunizieren. Gegenstände im Sinne dieser Definition können im gewerblichen Bereich alle Arten von Verbrauchs-, Anlage- oder Produktionsgütern sein.

Beispiele sind ein Handwerkzeug, das selbstständig seine Betriebsstunden und seinen technischen Zustand an eine zentrale Verwaltungssoftware überträgt oder eine Palette mit Halbfertigwaren, die sich über IoT-Komponenten orten lässt und die über ein Display eine schnelle Identifikation durch den Menschen zulässt. Von der Definition erfasst werden aber auch große, komplexe Anlagegüter wie Industrie- oder Bürogebäude, die durch die Ausstattung mit vernetzter Sensorik und Aktorik Teil des IoT werden.

Der Vorteil dieser neu zur Verfügung stehenden Daten kann zur Erzielung wirtschaftlicher Vorteile genutzt werden. Um dies zu erreichen, werden i.d.R. bereits zuvor existierende IT-Systeme oder technische Komponenten mit den neuen IoT-Daten angereichert, um organisatorische Prozesse oder technische Regelkreisläufe zu optimieren.

2. Entwicklungen der jüngsten Zeit

Grundlage der stark zunehmenden Verbreitung von IoT-Komponenten sind miniaturisierte Baugruppen, die auf neuen, leistungsstarken und energieeffizienten Übertragungstechnologien basieren. Übertragungsprotokolle wie Bluetooth Low Energy (BLE) oder ZigBee im Kurzstreckenbereich und sog. LPWAN-Technologien („Low Power Wide Area Network“) für die Überbrückung langer Distanzen ermöglichen den Einsatz von Funksensorik und -Aktorik auch dort, wo er früher nicht denkbar war.

Auch auf der Software-Seite haben sich Vereinfachungen ergeben. Es steht teils lizenzkostenfrei verfügbare Open-Source-Software für die Weiterverarbeitung der Daten und die Steuerung von IoT-Aktorik zur Verfügung.[5]

3. Einsatzgebiete von IoT-Technologien im gewerblichen Bereich

Die folgende Aufzählung von Anwendungsfeldern ist nicht abschließend, sondern soll beispielhaft die Möglichkeiten aufzeigen, die durch den Einsatz vernetzter Sensorik und Aktorik bestehen. Sie sind teilweise auch Ausgangspunkt der später behandelten Praxisfälle.

a) Energiemanagement in Gebäuden

Ein vollständig digitalisiertes Gebäude ermöglicht u.a. im energetischen Bereich Optimierungen mit kurzer Amortisationszeit. So können Heizkörper bei gekippten Fenstern deaktiviert, Besprechungsräume nur bei Bedarf beleuchtet und beheizt und die Dimmung der Beleuchtungen von Verkehrswegen anhängig von der Helligkeit des Tageslichtes geregelt werden. Zudem ist es möglich, Anlagen zur Erzeugung und Speicherung Erneuerbarer Energie („EE-Anlagen“) optimal zu steuern. Auch eine Steigerung des Benutzerkomforts, z.B. durch personenbezogene Behaglichkeitssteuerung in wechselnd genutzten Räumlichkeiten, ist umsetzbar. Schließlich ist auch die Erfüllung gesetzlicher Analyse- und Berichtspflichten leichter möglich, wenn die Daten hierzu automatisiert erzeugt und gespeichert werden.

b) Management mobiler Anlagegüter

Mobile Anlagegüter wie z.B. Gabelstapler, Handwerkzeuge etc. können bei Einsatz entsprechender IoT-Systeme umfassend überwacht werden. So kann jedes ausgerüstete Asset rechtzeitig vor Ablauf des herstellerseitig vorgeschriebenen Inspektionsintervalls zur Wartung eingeplant werden. Im Falle eines Diebstahls kann man es orten und ggf. aus der Ferne deaktivieren. Technische Anomalien können gemeldet und ein Ausfall des Gerätes mit Folgeschäden und -kosten vermieden werden. Über ein automatisiertes Reporting der Nutzung kann das interne Rechnungswesen ohne zusätzlichen Zeitaufwand z.B. bei der Ermittlung einer realitätsnahen kalkulatorischen Abschreibung Unterstützung erhalten.

[5] Übersicht aktueller Open-Source-IoT-Plattformen: *Domínguez-Bolaño/Campos et al.*, An overview of IoT architectures, technologies, and existing open-source projects (https://www.sciencedirect.com/science/article/pii/S254266052200107X, abgerufen am 17.03.2024) (s. Abschnitt 3.2).

c) Optimierungen in der Intralogistik

In Produktionsbetrieben bieten smarte Produktionsgüter, ausgestattet mit mobilen Ortungsmodulen und von Menschen lesbaren Displays, Möglichkeiten der Prozessoptimierung. So kann eine Palette mit Halbfertigzeugen jederzeit im Prozess geortet und z.B. das Ergebnis von Qualitätskontrollen direkt mit der Palette verknüpft werden. Das Display am IoT-Modul zeigt bei Bedarf automatisch die Sperrung der Ware aus Qualitätsgründen an und die vernetzte ERP-Software veranlasst den Intralogistiker, die Ware der Nachbearbeitung zuzuführen.

4. Kostenverfall beim Einsatz von Gebäudesensorik

In den letzten 10 Jahren hat bei der Digitalisierung von Gebäuden eine stetige Reduktion der dafür notwendigen Investitionen stattgefunden. Diese Entwicklung ist auf zwei Ursachen zurückzuführen.

Zum einen ist durch die Massenproduktion von IoT-Geräten der Preis pro Einheit gesunken. Zum anderen kann durch den Einsatz von Funktechnologien wie BLE, ZigBee, LoRa oder WLAN eine Datenverkabelung von IoT-Geräten, die oftmals ein Mehrfaches des eigentlichen Sensors kostet, entfallen und es muss nur noch die Stromversorgung sichergestellt sein. Ist ein Batteriebetrieb möglich, weil eine IoT-Einheit nur z.B. alle 5 Minuten einen Temperaturwert übertragen muss, kann eine Verkabelung vollständig entfallen und der Investitionsaufwand für die Anschaffung sinkt weiter.

II. Rechtliche Grundlagen zum Beschäftigtendatenschutz

Bis zum heutigen Tag gibt es trotz der erkannten Notwendigkeit und einiger Anläufe kein „Beschäftigtendatenschutzgesetz“.[6] Die Gesetze und Verordnungen zum allgemeinen Datenschutz wirken daher in Arbeitsverhältnisse hinein. Die wesentlichen Regelungen zum Beschäftigtendatenschutz werden im Folgenden erwähnt.

1. Datenschutz-Grundverordnung (DSGVO)

Die seit Mai 2018 geltende Datenschutz-Grundverordnung (DSGVO) genießt als EU-Verordnung rechtlichen Vorrang vor nationalen Regelungen.[7] Sie setzt einen umfassenden rechtlichen Rahmen für die Sammlung und Verarbeitung personenbezogener Daten. Jedoch lässt sie über kontextspezifische Öffnungsklauseln auch

[6] Zu den gesetzgeberischen Aktivitäten im Beschäftigtendatenschutz: *Düwell*, in: *Weth* et al., Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 9 Rn. 25 ff.
[7] *Ruffert*, in: *Calliess* et al., EUV/AEUV, Art. 1 AEUV [EUV und AEUV] Rn. 16.

Spielräume für nationale Regelungen. Dazu gehört gem. Art. 88 DSGVO auch die Datenverarbeitung im Beschäftigungskontext. Deutschland hat von der Möglichkeit der nationalen Ausgestaltung im Rahmen des Bundesdatenschutzgesetzes Gebrauch gemacht.

2. Bundesdatenschutzgesetz (BDSG)

Das BDSG definiert neben Durchführungsbestimmungen der DSGVO-Vorschriften auch deutsche Normen zum Datenschutz in den Bereichen, die den nationalen Gesetzgebern über die o.g. Öffnungsklauseln optional zur spezifischen Gestaltung übertragen wurden. Für den Bereich des Beschäftigtendatenschutzes fanden solche nationalen Regelungen Eingang in § 26 BDSG.

§ 26 Abs. 1 S. 1 BDSG ist nach h.M. jedoch nach einem Urteil des EuGH[8] nicht mehr anzuwenden.[9] Zwar bezog sich das Urteil auf § 23 Abs. 1 S. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG), die fragliche Norm ist allerdings weitgehend identisch mit § 26 Abs. 1 S. 1 BDSG, dessen Anwendbarkeit somit ebenfalls von der Entscheidung betroffen ist.

Aus diesem Grund werden bei den nachfolgenden Erwägungen zur Zulässigkeit von Datenspeicherungen und -Verarbeitungen die Rechtsgrundlagen der DSGVO herangezogen. Regelungen des BDSG werden nur verwendet, sofern sie nach h.M. noch anwendbar sind.

3. Betriebsverfassungsgesetz (BetrVG)

Auch das BetrVG enthält Regelungen, die Berührungspunkte zum Datenschutz in Beschäftigungsverhältnissen aufweisen. Dies beginnt bei § 80 Abs. 1 Nr. 1 BetrVG, der den Betriebsrat zur Überwachung der Einhaltung gesetzlicher Vorschriften, hier der DSGVO und dem BDSG, verpflichtet. § 80 Abs. 2 S. 1 und 2 BetrVG gewährleisten den Anspruch auf Aushändigung der dafür nötigen Informationen durch das Unternehmen.

Eine im vorliegenden Kontext möglicherweise entscheidende Norm ist § 87 Abs. 1 Nr. 6 BetrVG, der ein Mitbestimmungsrecht des Betriebsrates bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“, vorsieht. Sollte dies

[8] EuGH, Urt. v. 30.03.2023 - C-34/21, ECLI:EU:C:2023:270, NZA 2023, 487 Rn. 82 - Hauptpersonalrat.

[9] *Kaufmann/Wegmann et al.*, NZA 2023, 740; *Maschmann*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, § 26 BDSG Rn. 2, 2a.BDSG

auf die geschilderten Usecases zutreffen, würde als zusätzliche Bedingung für die Inbetriebnahme der Systeme hinzukommen, dass der Betriebsrat ihrer Einführung zustimmt.

Grenzen setzt das das kollektive Arbeitsrecht dem Verhandlungsspielraum von Betriebsräten in § 75 Abs. 2 BetrVG dort, wo Persönlichkeitsrechte von Beschäftigten berührt werden. Dies betrifft auch Belange des Datenschutzes.[10]

B. Usecases aus der Praxis

I. Fall 1: Gebäudedigitalisierung zum Energiemanagement

1. Problemstellung

Die E GmbH ist eine mittelständische Unternehmensgruppe mit ca. 600 Beschäftigten. Gestiegene Energiekosten sowie gesetzliche Vorgaben in Form der §§ 8 und 9 des Energieeffizienz-Gesetzes (EnEfG) haben bei der Geschäftsleitung Handlungsbedarf in Sachen Energiemanagement erkennen lassen. Zudem ist im Kodex des Unternehmens eine allgemeine Selbstverpflichtung zu nachhaltigem Wirtschaften verankert, die zur Einhaltung jährlich neu definierter Umweltziele führen soll.

Aus diesem Grund werden durch ein spezialisiertes Ingenieurbüro der energetische Status Quo ermittelt und ein Maßnahmenkatalog zum Energiemanagement gem. DIN EN 17463 ausgearbeitet.

Für die Verwaltungszentrale mit rund 120 Arbeitsplätzen ist das Ergebnis, dass die Voraussetzungen für ein Energiemanagement bauseitig gegeben sind. Die gute Wärmedämmung und die bereits vollständig auf LED-Technologie umgerüstete Beleuchtung lassen zwar wenig Spielraum für sinnvolle Verbesserungen auf der Ebene der Effizienz des Gebäudes. Erhebliches Potenzial weist das erstellte Gutachten jedoch bei der bedarfsorientierten Steuerung des Verbrauchs aus. Aus diesem Grund soll das Gebäude in den Bereichen Heizung, Klimatisierung und Beleuchtung vollständig digitalisiert werden. Anhand von Rechenmodellen und Erfahrungswerten eines herangezogenen wissenschaftlichen Institutes ist eine Senkung des Energieverbrauches im Bereich Strom von 20% und für die mit Gas betriebene Heizung von 15% zu erwarten. Die Modellierung ergibt weiterhin, dass etwa 25% der gesamten Ersparnis im Zusammenhang mit personalisierten Funktionen erreicht werden, z.B. durch die Beheizung oder Kühlung von Räumen in

[10] *Raif*, in: *Kramer*, IT-Arbeitsrecht, § 3 Rn. 3.

Abhängigkeit von Raumbelegungskalendern und die automatische Anpassung an persönliche Einstellungen.

Es ergibt sich eine Amortisationszeit von ca. 6 Jahren, abhängig von der weiteren Entwicklung der Energiepreise. Erweitert wird die Zieldefinition schließlich um den Faktor des Komforts, daher wird auch die Expertise der Fachabteilung „Thermische Behaglichkeit, Modelle und Simulation“ des beauftragten Institutes genutzt.

2. Lösungsansatz

Nach eingehender Marktstudie auf dem Markt der industrietauglichen Smart-Building-Server verbleibt ein Produkt eines neu agierenden Herstellers, das die gewünschten Funktionen bietet und die sonstigen Vorgaben aus dem erstellten Lastenheft erfüllt. Der Server soll mit der nachzurüstenden Gebäudetechnik-Hardware für die Licht- und Klimasteuerung verbunden werden. Mit der Umsetzung des Projektes wird die interne IT-Abteilung beauftragt.

Um die prognostizierten Kennzahlen zur Energieeinsparung zu erreichen, sind folgende Funktionalitäten geplant:

a) Heizung und Klimatisierung

Die einzelnen Räume des Gebäudes sollen zukünftig nicht mehr durchgehend auf Temperatur gehalten, sondern abhängig von der Nutzung geregelt werden. Hierbei wird unterschieden zwischen öffentlichen Räumen wie z.B. der Kantine oder Konferenzräumen einerseits sowie Büros, die von jeweils vier Personen genutzt werden, andererseits.

Öffentliche Räume sollen nach den Regel-Arbeitszeiten sowie zusätzlich anhand ihrer Belegung im Ressourcenkalender vorgeheizt bzw. -gekühlt werden. Unterstützt werden soll das System durch eine kamerabasierte Bewegungserkennung in der Kantine sowie im Mehrzweckraum, der für unterschiedliche Veranstaltungen genutzt wird. Damit soll die Raumtemperatur abhängig vom Bewegungsprofil der anwesenden Personen gesteuert werden, ein Ergebnis aus der langjährigen Forschung des wissenschaftlichen Institutes. Bewegen sich nämlich Personen im Raum, z.B. bei einer Festivität oder dem monatlich stattfindenden „After Work Get Together“, liegt die Wohlfühltemperatur rund 3 Grad Celsius niedriger als bei sitzenden Personen und 1,5 Grad Celsius niedriger als bei stehenden. Die Auswertung der Bilder wird automatisiert im Prozessor der Kamera vorgenommen, dessen Software eine KI-gestützte Komponente zur Erkennung der Bewegungsprofile der

erfassten Personen besitzt. Zur laufenden Verbesserung der KI-Erkennungsqualität werden Videosequenzen immer dann zum Hersteller-Server übertragen, wenn die Kamera-Software den Bewegungszustand einer Person, ob sie also steht, sitzt oder sich bewegt, mit einer Wahrscheinlichkeit von weniger als 80% erkennen kann. Beim Hersteller wird manuell durch Menschen das KI-generierte Ergebnis pro erfasster Person korrigiert bzw. bestätigt. Dies geschieht aus Kostengründen in einer Niederlassung in Asien. Schließlich werden den Kameras der Kunden, hier der E GmbH, optimierte Algorithmen zurückgeliefert, so dass die Erkennungsqualität stetig verbessert wird.

Büros sollen zukünftig je nach persönlichem Empfinden temperiert werden. Dazu kann über eine App auf dem Diensthandy die persönliche Wohlfühltemperatur innerhalb definierter Grenzen eingestellt werden. Bei Anwesenheit wird diese automatisch vorgewählt. Ob jemand an seinem Schreibtisch sitzt, ermittelt die zentrale Steuerungs-Software anhand eines speziellen Anwesenheitssensors am Schreibtisch. Nutzen mehrere Personen gleichzeitig ein Büro, wird automatisch der Mittelwert der persönlichen Sollwerte eingestellt.

b) Beleuchtung

Die Beleuchtung soll zukünftig ebenfalls bedarfsgerecht gesteuert werden.

In Büros wird dazu, sobald Personen über einen kombinierten Bewegungs- und Helligkeits-Sensor erfasst werden, das Raumlicht automatisch auf den in der entsprechenden technischen Norm für Verkehrsflächen vorgeschriebenen Helligkeitswert eingestellt. Das bedeutet für helle Tage mit viel Außenlicht, dass die Beleuchtung automatisch ausgeschaltet wird, an dunkleren Tagen wird nur der nötige Anteil an künstlicher Beleuchtung per Dimmfunktion zugemischt, so dass der Energiebedarf für die Beleuchtung minimiert wird.

Zusätzlich werden die einzelnen Schreibtisch-Arbeitsplätze individuell beleuchtet. Da jeder Arbeitsplatz über eine eigene, dimmbare Hängeleuchte ausgestattet ist, kann ihre Helligkeit nach Bedarf für die eigenen Schreibtisch-Arbeitsplätze angepasst werden; auch hier wird über den o.g. Anwesenheitssensor am Schreibtisch erfasst, wenn dieser besetzt ist. Der Server speichert auch in diesem Fall den individuellen Komfortwert ab und bei der nächsten Anwesenheit wird diese Anpassung automatisch abgerufen. Wird der Schreibtisch verlassen, schaltet der Server die Beleuchtung des Arbeitsplatzes aus.

In öffentlichen Bereichen und insbesondere Verkehrswegen wird ausschließlich mit den genormten, vorgeschriebenen Helligkeitswerten gearbeitet. Individuelle Anpassungen sind nicht vorgesehen.

Eine historische Aufzeichnung der Anwesenheitsdaten findet nicht statt. Direkt nach dem Auslösen einer Aktion, z.B. dem Einstellen einer neuen Zieltemperatur oder Helligkeit, werden die entsprechenden Sensordaten aus der Datenbank gelöscht.

3. Reaktion nach Erstvorstellung

Die Geschäftsleitung stellt ihrer Verpflichtung gem. § 80 Abs. 2 BetrVG folgend das geplante Projekt dem Betriebsrat vor, dem der Datenschutzbeauftragte ebenfalls angehört. Alle Anwesenden sind vom Einsparpotenzial und den Komfortfunktionen begeistert, jedoch mischen sich auch Bedenken bezüglich des Datenschutzes in die Diskussion. Eine Datenschutz-Betriebsvereinbarung liegt nicht vor. Man kommt überein, das Vorhaben im Rahmen einer Datenschutz-Folgenabschätzung gem. Art. 35 Abs. 1 DSGVO extern begutachten zu lassen.

II. Fall 2: Personenortung in Gefahrenbereichen

1. Problemstellung

Die M AG ist eine mittelständischer Zulieferer für die Automobilindustrie. Hergestellt werden u.a. speziell beschichtete Blechteile, die in Bereichen mit hohen Anforderungen an Schallabsorption und Brandschutz in Nutzfahrzeugen verbaut werden. Am einzigen Produktionsstandort arbeiten etwa 600 Beschäftigte in drei Schichten. Bei der M AG kam es innerhalb eines Jahres zu zwei Ereignissen, die Handlungsbedarf im Bereich des Arbeitsschutzes erkennen lassen.

a) Beinahe-Unfall im Rohwaren-Lager

Im Bereich der ca. 2.500 m² großen Rohwarenlagerung kam es zu einem Beinahe-Unfall. Die Haltemechanik des Vakuumkranes, der Bleche von Stapeln entnimmt und Shuttle-Fahrzeuge bestückt, versagte im laufenden Betrieb. Bei einer Minuten zuvor erfolgten Wartung kam es zu einem Fehler durch menschliches Versagen. Im vorliegenden Fall fiel ein 100 kg schweres Blech aus zehn Metern Höhe herab. Ein Mitarbeiter, der eine zyklisch erforderliche Qualitätskontrolle der korrosionsanfälligen Rohwaren im Gefahrenbereich durchführte und leichtfertig vermutete, der

Kran sei noch längere Zeit im Wartungsmodus, wurde nur um wenige Meter verfehlt.

Eine Recherche zu den Gründen, warum der Mitarbeiter sich trotz des arbeitenden Kranes noch im Lager aufhalten konnte, ergab, dass zuvor aufgrund der Unübersichtlichkeit des Lagerbereiches nicht mit letzter Sicherheit festgestellt werden konnte, ob sich bei der Reaktivierung des Kranes noch jemand im Lager aufhielt. Die Personentür zum Kranlager deaktiviert den Kran zwar bei einer Öffnung sofort, jedoch wurde sie durch den Mitarbeiter zur Zeit der laufenden Wartung genutzt, so dass diese Sicherheitseinrichtung nicht greifen konnte.

Der Zugang zum Lagerbereich ist darüber hinaus nicht vollständig abzusichern, da dieser zwar eingezäunt ist, jedoch Öffnungen für die beiden Logistik-Shuttles existieren, die Waren zu den Verarbeitungsmaschinen bringen.

Eine Videoüberwachung des Lagers scheidet aus, da es vollautomatisiert und mit dynamisch vergebenen Stellplätzen von der Logistiksoftware bewirtschaftet wird. Es entstünden je nach Anordnung der Lagerplätze also immer wieder tote Winkel, die nicht überwacht werden können.

Der Vorfall wurde von der Sicherheitsbeauftragten des Unternehmens dokumentiert und der Geschäftsleitung gemeldet. Diese beschließt, das Beinahe-Ereignis zum Anlass für eine organisatorische und technische Überarbeitung ihres Sicherheitskonzeptes im Lager zu nehmen. Dies schließt auch eine offene Kommunikation mit der zuständigen Berufsgenossenschaft ein.

b) Lange Suchzeiten im Evakuierungsfall

Im Bereich der Verarbeitungsanlage, die mit chemischen Prozessen die Spezialbeschichtung auf die Bleche aufschäumt, kam es zu einem Prozessfehler, der mit Gasaustritt und Rauchentwicklung verbunden war. Bei der Räumung des Gebäudes mussten die evakuierten Personen ausgezählt und manuell mit den Daten der Zeiterfassung sowie der Besucherliste abgeglichen werden. Nachdem sich herausgestellt hatte, dass zwei Personen vermisst wurden, dauerte deren Evakuierung nochmals einige Zeit, da wegen der Sichtbehinderungen lange nach ihnen gesucht werden musste. Sie trugen Gas- und Rauchvergiftungen davon und konnten erst nach längerer Genesung wieder aus einer Rehabilitationsmaßnahme entlassen werden.

2. Lösungsansatz

Sowohl die Berufsgenossenschaft als auch die Versicherung, bei der die M AG einen Vertrag für die finanzielle Versorgung ihrer Beschäftigten für Unfälle mit Personenschaden abgeschlossen hat, bitten aufgrund der Ereignisse unabhängig voneinander um einen Gesprächstermin zum Thema Risikomanagement im Arbeitsschutz. Das Gewerbeaufsichtsamt hat ebenfalls angekündigt, bei der in Kürze anstehenden regelmäßigen Begehung die Vorfälle zu thematisieren. Aus diesem Grund entschließt sich die Geschäftsleitung auch in diesem Fall, proaktiv ein Gesamtkonzept zur Vermeidung solcher Unfälle sowie zur Verringerung ihrer Folgen zu entwickeln.

Ein Teil der Pläne befasst sich mit der Ortung von Personen in Gefahren- und Unfallbereichen. Nach eingehender Marktrecherche zum bestehenden Technologiestand durch die IT-Abteilung fokussiert sich das Interesse auf ein System, das alle im Produktionsgebäude anwesenden Personen in Echtzeit ortet. Dieses arbeitet auf Bluetooth-Low-Energy-Basis (BLE) und verwendet die sog. AOA („Angle of Arrival“)-Technologie, um spezielle Bluetooth-Geräte in Räumen orten zu können.[11] Solche Geräte, genannt „BLE-Tags“, gibt es in Form von Karten zum Umhängen oder als Armbänder.

An der Decke des Produktionsgebäudes werden in einem Raster von ca. 8 m Basisstationen installiert, die die Signale dieser Tags empfangen. Das Besondere am AOA-Prinzip ist, dass jede Basisstation nicht nur die Identifikationsnummer („ID“) des Tags auswertet, sondern auch den Winkel, aus dem sein Signal empfangen wird. So reichen bereits Daten von drei Basisstationen aus, um den Standort eines Tags und somit des Menschen, der es bei sich trägt, auf 50 cm genau ermitteln zu können. Die zugehörige Software auf dem firmeneigenen Server zeichnet alle ermittelten Standorte im zeitlichen Abstand von einer Sekunde auf und ist in der Lage, zu jeder Zeit den Standortverlauf sowie den aktuellen Ort jedes BLE-Tags und somit jeder Person sichtbar zu machen.

Geplant ist für die Zukunft, dass jeder Beschäftigte sein persönliches BLE-Tag mit sich führt. Sobald bei aktivem Kran eine Person in dessen Bewegungsbereich geortet wird, bewegt sich dieser aus dem Gefahrenbereich heraus, dabei wird die Position der georteten Person weitläufig umfahren. Er lässt sich erst wieder reaktivieren, wenn sich kein BLE-Tag und somit kein Mensch mehr im Lagerbereich befindet.

[11] Skizze zur Funktion s. Anhang 2

Eine automatisierte Durchsage mit deutlich erkennbarer optischer Signalisierung des Alarmzustandes soll die betroffenen Personen animieren, den Bereich schnell zu verlassen. Mit dieser Lösung sollen Gefahren durch herabfallende Lasten vollständig eliminiert und Standzeiten verringert werden. Zusätzlich kann im System nachträglich ausgewertet werden, wer geortet wurde, so dass eine Nachschulung der Beschäftigten zur Sensibilisierung bezüglich des Arbeitsschutzes durchgeführt werden kann.

Bezüglich der Auffindbarkeit von Personen im Evakuierungsfall kann mit der Systemfunktionalität innerhalb weniger Sekunden festgestellt werden, wer sich noch im Produktionsbereich befindet und vor allem wo genau sein Aufenthaltsort ist. Dies ermöglicht die gezielte Suche nach verbliebenen Personen im Evakuierungsfall. Dazu stehen für diese Situationen entsprechende Industrie-Tablets an den Zugängen für die Rettungskräfte bereit, mit deren Hilfe sie innerhalb des Gebäudes zu den Punkten geleitet werden, an denen Personen geortet wurden.

Die Aufzeichnung der Ortungsdaten findet in einer integrierten Datenbank statt. Standardmäßig werden die ältesten Daten rotierend gelöscht, wenn die Datenbank eine Größe von 80% des Datenträgersystems erreicht hat.

3. Reaktion nach Erstvorstellung

Auch für dieses Vorhaben findet eine Vorstellung des Projektes gegenüber dem Betriebsrat und dem Datenschutzbeauftragten statt. Zwar sehen beide Instanzen die Notwendigkeit einer Lösung für die Gefahren, die bei den beiden Vorfällen offensichtlich geworden sind. Andererseits besteht die Befürchtung, dass das System auch zu Überwachungszwecken missbraucht werden könnte, zumal der Personalleiter, der als Mitglied der Geschäftsführung gleichzeitig der Vorgesetzte der IT-Abteilung ist, als „Kontrollfreak“ gilt.

Auch in diesem Fall wird ein Gutachten gem. Art. 35 Abs. 1 DSGVO beauftragt. Im Falle rechtlicher Unzulässigkeit von Teilfunktionalitäten sollen einwandfreie Alternativen ausgearbeitet werden.

C. Datenschutzrechtliche Problembereiche und einschlägige Normen

I. Gemeinsame Betrachtungen für Fall 1 und 2

1. Speicherung personenbezogener Daten auf den Anwendungsservern

Fraglich ist zunächst, ob es zur Speicherung bzw. Verarbeitung personenbezogener Daten auf den Anwendungsservern käme.

Personenbezogene Daten sind gem. Art. 4 Nr. 1 DSGVO definiert als „alle Informationen, die sich auf eine […] identifizierbare Person beziehen […]". Als identifizierbar gilt eine natürliche Person nach dieser Norm dann, wenn sie u.a. „mittels Zuordnung zu einer Online-Kennung […] identifiziert werden kann."

Für Fall 1 ist dies gegeben, da die beim Smart-Building-Server die Login-Kennung eines jeden Beschäftigten seine Firmen-E-Mail-Adresse ist. Weil der Server zur Bereitstellung seiner Funktionen neben dem Klartext-Vor- und Nachnamen zusätzlich eine Vielzahl weiterer Daten zu jeder Person speichert, ist vom Tatbestand der Speicherung personenbezogener Daten auf dem Smart-Building-Server auszugehen.

In Fall 2 ist im Konzept, das dem Betriebsrat und der Datenschutzbeauftragten vorgestellt wurde, jedem Beschäftigten im Produktionsbereich ein festes BLE-Tag zugeordnet, das zwingend beim Betreten des Gebäudes zu tragen ist. Auch hier werden Personendaten wie Klarnamen, E-Mail-Adresse und weitere Details in der Nutzerdatenbank gespeichert. Somit ist auch in Fall 2 von der Speicherung personenbezogener Daten auszugehen.

Zwischenergebnis: In beiden Fällen werden personenbezogene Daten gespeichert bzw. verarbeitet.

Zu prüfen ist daher in beiden Fällen, ob die Speicherung und ggf. Verarbeitung personenbezogener Daten auf den jeweiligen Servern nach den einschlägigen Normen zulässig ist und ob möglicherweise eine Zustimmung des Betriebsrates nach kollektivrechtlichen Regelungen erforderlich ist.

In Frage kommen die DSGVO und das BDSG als Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Dazu müssten sie im vorliegenden Fall

anwendbar sein. Dies ist der Fall, wenn für eine Norm ihr räumlicher und sachlicher Anwendungsbereich eröffnet sind.

a) Anwendbarkeit DSGVO

Für die DSGVO gilt diesbezüglich, dass ihr sachlicher Anwendungsbereich gem. Art. 2 Abs. 1 DSGVO durch die automatisierte Verarbeitung der Daten der Beschäftigten auf den Servern erfüllt ist. Der Personenbezug ergibt sich im Fall „Smart Building" aus den personenbezogenen Server-Accounts, im Fall „Ortung von Beschäftigten" aus der festen Verknüpfung zwischen BLE-Tag und Person. Der räumliche Anwendungsbereich i.S.d. Art. 3 Abs. 1 DSGVO ist durch den Standort beider Unternehmen in Deutschland ebenso gegeben. Auch die Begriffsbestimmung in Art. 4 Nr. 7 DSGVO („Verantwortlicher") trifft auf die Unternehmen im vorliegenden Fall zu.

b) Anwendbarkeit BDSG

Das BDSG definiert in §§ 1 S. 2 Alt. 1, 4 Nr. 1 beide Fälle als ebenso einschlägig. Zudem spezifiziert es in § 26 Abs. 8 die betroffenen Personen, hier jeweils die Beschäftigten der Unternehmen.

Zwischenergebnis: Sowohl die DSGVO als auch das BDSG sind in beiden Fällen anwendbar.

2. Zulässigkeit der Speicherung bzw. Verarbeitung personenbezogener Daten auf den Anwendungsservern

Im nächsten Schritt ist die Zulässigkeit der Datenverarbeitung auf dem Server zu betrachten. Dazu müsste ein entsprechender Erlaubnistatbestand vorliegen, denn sowohl die DSGVO als auch das BDSG folgen dem Prinzip des Verbotes mit Erlaubnisvorbehalt.[12] Erlaubnistatbestände können auf verschiedenen Wegen entstehen, die im Folgenden betrachtet werden sollen.

a) Art. 6 Abs. 1 a) DSGVO – Freiwillige, individuelle Zustimmung aller Beschäftigten

Es besteht die Möglichkeit, dass die Beschäftigten nach Art. 6 Abs. 1 a) DSGVO jeweils individuell ihre freiwillige Einwilligung zur Verarbeitung der im

[12] *Wolff*, in: *Wolff/Brink*, Datenschutzrecht, Bereichsspezifischer Datenschutz, DS-GVO, BDSG, Syst. A Rn. 18.1, 18.2.

digitalisierten Gebäude entstehenden Daten erteilen. Im Beschäftigungskontext sind hier aufgrund des bestehenden Ungleichgewichtes der Verhandlungspositionen zwischen Beschäftigten und Unternehmern jedoch besondere Anforderungen an die Wirksamkeit einer solchen Einwilligung zu stellen. Wurde vor der Einführung der DSGVO und der heutigen Fassung des BDSG sogar gelegentlich die Wirksamkeit der freiwilligen Zustimmung als gänzlich ausgeschlossen betrachtet[13], so gilt heute unter Verwendung der Anhaltspunkte in Erwägungsgrund 43 DSGVO die Abwägung im Einzelfall als angezeigt.[14]

Dass die freiwillige Zustimmung aller Beschäftigten gem. Art. 6 Abs. 1 a) DSGVO zumindest bei prozessrelevanten sowie kostenintensiven Systemen als alleinige Rechtsgrundlage kritisch zu betrachten ist, liegt an ihrer rechtlichen Fragilität. So reichen bereits ein einziger Widerruf gem. Art. 7 Abs. 3 S. 1 DSGVO oder die Verweigerung einer Einwilligung durch einen neu eingestellten Beschäftigten aus, um den Betrieb eines Systems möglicherweise gesetzeswidrig werden zu lassen. Zumindest jedoch würde mangels vollständiger Erfassung aller Mitarbeitenden der Zweck eines sicherheitsrelevanten Systems wie in Fall 2 ad absurdum geführt.

Aus diesem Grund sollen vertiefende Betrachtungen zur freiwilligen Einwilligung gem. Art. 6 Abs. 1 a) DSGVO im vorliegenden Kontext ausgespart werden.

b) Art. 88 Abs. 1 S. 1 Alt. 2 DSGVO - Kollektivrechtliche Zustimmung

Eine weitere Möglichkeit, die in den geplanten Systemen anfallenden Daten legal zu verarbeiten, bietet gem. Art. 88 Abs. 1 S. 1 Alt. 2 DSGVO eine Betriebsvereinbarung. Gem. § 77 Abs. 4 S. 1 BetrVG entfaltet diese unmittelbare rechtliche Wirkung.[15] In beiden Fällen könnte also durch eine solche Vereinbarung eine Rechtsgrundlage zur Speicherung und Verarbeitung personenbezogener Beschäftigtendaten entstehen.

Allerdings hat diese Wirksamkeit Grenzen; dabei wird in der Literatur vor allem das Thema behandelt, ob in einzelnen Regelungen der Schutzstandard der DSGVO unterschritten werden könne, sofern das Niveau insgesamt durch schärfere Regelungen an anderer Stelle aufrecht erhalten wird, ob er nie unter-, jedoch

[13] *Conrad/Treeger*, in: *Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, § 34 Rn. 339.

[14] *Stemmer*, in: *Wolff/Brink*, Datenschutzrecht, Bereichsspezifischer Datenschutz, DS-GVO, BDSG, Art. 7 Rn. 53; *Conrad/Treeger*, in: *Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, Art. 34 Rn. 471 ff.

[15] *Gola*, Handbuch zum Arbeitnehmerdatenschutz, Kap. 12 Rn. 1926 ff.

überschritten werden dürfe oder ob gar exakt das in der DSGVO vorgesehene Schutzniveau umzusetzen sei („Vollharmonisierung“).[16] Vertrat der EuGH früher die Position der Vollharmonisierung[17], rückte er von dieser Haltung in seinem Urteil vom 30.03.2023 ab und erlaubt den Mitgliedsstaaten (und somit indirekt über Art. 88 Abs. 1 S. 1 Alt. 2 DSGVO auch kollektivrechtlichen Parteien), für Beschäftigte auch höhere Schutzstandards als im DSGVO vorgesehen zu vereinbaren.[18]

Weiterhin zieht auch das BetrVG selbst Grenzen; so gibt § 75 Abs. 2 S. 1 BetrVG vor, dass nicht nur der Arbeitgeber, sondern auch der Betriebsrat die „freie Entfaltung der Persönlichkeit zu schützen und zu fördern“ haben. Dies bezieht auch Überwachungs- und Kontrollmaßnahmen mit ein, denen der Betriebsrat nicht zustimmen dürfte, wenn sie aus gesetzlicher Sicht im Hinblick auf die Persönlichkeitsrechte der Beschäftigten unzulässig wären.[19] Letztendlich ergibt sich jedoch hieraus die gleiche Rechtsfolge wie im vorstehenden Absatz beschrieben, dass nämlich gesetzliche Schutzstandards nicht durch Betriebsvereinbarungen unterlaufen werden können.

Sofern die vorstehend beschriebenen Vorgaben in eine Betriebsvereinbarung aber einbezogen würden, wäre sie grundsätzlich ein geeignetes Instrument zum legalen Betrieb der geplanten Systeme. Zudem wäre mit einer Betriebsvereinbarung auch das Mitbestimmungsrecht des Betriebsrates gem. § 87 Abs. 1 Nr. 6 BetrVG bereits abgehandelt, das bei einer ausschließlich auf den Datenschutzvorschriften basierenden Betrachtung separat zu berücksichtigen wäre.

Allerdings gibt es auch Gründe, eine Betriebsvereinbarung als Grundlage für ein bestimmtes einzuführendes System aus Sicht des Unternehmens kritisch zu betrachten. Wenn nämlich das einzuführende System die gesetzlich vorgegebenen Datenschutz-Standards einhielte, bedürfte es keiner gesonderten Betriebsvereinbarung, um den Betrieb zu legalisieren. Erreichte das System dagegen auch nur in Teilen nicht die gesetzlich vorgegebenen Standards, könnte nach der aktuell vom EuGH vertretenen Meinung auch eine Betriebsvereinbarung keine Rechtsgrundlage für seinen Betrieb schaffen, da eine Unterschreitung der europäischen Standards nicht durch einzelne Mitgliedsstaaten legalisiert werden kann.[20] Dies gälte auch für eine

[16] *Gola*, Handbuch zum Arbeitnehmerdatenschutz, Kap. 12 Rn. 1960 ff.
[17] EuGH, Urt. vom 24.11.2011 - C-468/10 -, NZA 2011 (1409 Rn. 47) - ASNEF.
[18] EuGH, Urt. v. 30.03.2023 - C-34/21, ECLI:EU:C:2023:270, NZA 2023, 487 Rn. 51, 78 - Hauptpersonalrat.
[19] *Kolbe*, in: *Dornbusch* et al., AR - Kommentar zum ges. Arbeitsrecht, § 75 BetrVG Rn. 18.
[20] Vgl. *König*, Beschäftigtendatenschutz in der Beratungspraxis, Teil VII. Rn. 232.

Betriebsvereinbarung, die aufgrund nationaler Gesetzgebung Befugnisse auf Betriebsräte und Unternehmen überträgt.

Zu beachten ist zudem in der Praxis, dass die Betriebsvereinbarung unter Ausschluss der ordentlichen Kündigungsmöglichkeit abzuschließen wäre.[21] Ansonsten bestünde das Risiko einer Kündigung gem. § 77 Abs. 5 BetrVG durch den Betriebsrat. Diese würde eine Gefahr für die Investitionssicherheit darstellen, wenn nämlich laufende Systeme wegen der Kündigung wieder außer Betrieb genommen oder nachträglich so angepasst werden müssten, dass sie den Bedingungen des Betriebsrates für eine Fortführung der Betriebsvereinbarung genügen würden.

In beiden geschilderten Usecases hat der Betriebsrat jedoch, zumindest in der seitens der Geschäftsleitung angedachten Funktionalität, ohnehin Bedenken hinsichtlich des Datenschutzes, so dass ohne Änderungen am Konzept keine Bereitschaft zum Abschluss einer entsprechenden Betriebsvereinbarung besteht.

c) Erlaubnistatbestand aus Art. 6 Abs. 1 b) Alt. 1, c), d), f) DSGVO

Eine dritte Möglichkeit, den Betrieb beider Projekte aus Sicht des Datenschutzes rechtskonform zu gestalten, wäre das Vorliegen eines gesetzlichen Erlaubnistatbestandes aus Art. 6 Abs. 1 b) Alt. 1, c), d) und/oder f) DSGVO.

Dabei muss innerhalb des Spannungsfeldes, bestehend aus dem Interesse der Beschäftigten am Schutz der persönlichen Daten, dem wirtschaftlichen Interesse des Unternehmens sowie den rechtlichen Verpflichtungen, denen es unterliegt, abgewogen werden.[22] Besonderes Augenmerk ist bei dieser Abwägung stets auf die Erforderlichkeit der Datenverarbeitung zu legen.[23]

Diese Aspekte sollen für beide beschriebenen Fälle und ihre jeweiligen Teilfunktionalitäten im Folgenden untersucht werden.

[21] dies ist möglich; vgl. *Gaul*, in: *Henssler*/*Willemsen*/*Kalb*, Arbeitsrecht, BetrVG § 77 Rn. 35.
[22] *Riesenhuber*, in: *Brink*/*Wolff*/*v. Ungern-Sternberg*, BeckOK Datenschutzrecht, DSGVO Art. 88 Rn. 74.
[23] *Heberlein*, in: *Ehmann*/*Selmayr*, Datenschutz-Grundverordnung, Art. 6 Rn. 28.

II. Fallbezogene Betrachtungen

1. Fall 1 – Smart Building

a) Mögliche Erlaubnistatbestände aus Art. 6 Abs. 1 b) Alt. 1, c), d), f) DSGVO

aa) Speicherung der Stammdaten der Beschäftigten

Bei der Speicherung personenbezogener Stammdaten wie Name, E-Mail-Adresse etc. könnte sich die E GmbH möglicherweise auf Art. 6 Abs. 1 c) oder f) DSGVO berufen.

Bzgl. Art. 6 Abs. 1 c) DSGVO müsste sie einer rechtlichen Verpflichtung unterliegen, diese Daten zu speichern. Das Gesetz, das dem Unternehmen eine solche Pflicht indirekt auferlegt, könnte hier das EnEfG sein. Dessen § 8 Abs. 1 verpflichtet die E-GmbH aufgrund ihres Energieverbrauches der letzten drei Jahre zur Einführung eines „Energie- oder Umweltmanagementsystem[s] gemäß Absatz 2 Satz 1 oder Satz 2“ EnEfG. § 8 Abs. 3 i.V.m. § 9 S. 1 Alt. 1 EnEfG fordert schließlich die Erstellung sich daraus ergebender Umsetzungspläne. Die Definition von Wirtschaftlichkeit gem. § 9 S. 2 ff EnEfG ist im Fall des vorliegenden Projektes erfüllt.

Allerdings reicht eine solche indirekte Verpflichtung nicht aus. Eine Berufung auf Art. 6 Abs. 1 c) DSGVO setzt voraus, dass diese Rechtsvorschrift dem Verantwortlichen, hier der E-GmbH, direkt die Pflicht zur Speicherung bzw. Verarbeitung auferlegt.[24] Das ist jedoch nicht der Fall; erst die von der E GmbH gewählte Art der Umsetzung der Rechtsvorschrift und zudem erst die Optimierung des Konzeptes durch die Personalisierung der Systemfunktionen erfordern die Speicherung der Personendaten.

Die E GmbH kann ihre Argumentation also nicht auf Art. 6 Abs. 1 c) DSGVO stützen.

Stattdessen könnte möglicherweise Art. 6 Abs. 1 f) DSGVO eine Rechtsgrundlage zur Personendatenspeicherung liefern. „Berechtigtes Interesse“ i.S.d. Norm könnten in diesem Fall die Verbesserung ihres wirtschaftlichen Ergebnisses und die Einhaltung der im Kodex abstrakt verankerten und der daraus jährlich konkret definierten Umweltziele sein.

[24] LSG Hessen 4. Senat, Beschl. v. 29.01.2020, L 4 SO 154/19 B, Rn. 13 (BeckRS 2020, 1442).

Um festzustellen, ob die Voraussetzungen des Art. 6 Abs. 1 f) DSGVO erfüllt sind, ist eine dreistufige Prüfung vorzunehmen.[25]

Die erste Stufe dieser Prüfung betrifft demnach im vorliegenden Fall die Frage, ob zum Zeitpunkt der Verarbeitung der Daten ein berechtigtes Interesse der E GmbH vorliegt. Dieses Interesse besteht fortwährend seitens der Firma in der modellier4ten zusätzlichen Energie-Einsparung, wie sie durch das beauftragte Ingenieurbüro bei der personalisierten Umsetzungsvariante errechnet wurde. Sie macht im Jahr für die E-GmbH einen Betrag von etwa 3.000,- EUR aus und entspricht, umgerechnet auf den aktuell bezogenen Primärenergie-Mix, mehreren Tonnen CO_2-Äquivalent. Das Ergebnis setzt sich also aus einem wirtschaftlichen Teil, nämlich der Kostenersparnis, und einem aus Sicht der Firma ideellen Teil, der Emissionsverringerung, zusammen. Beide Aspekte werden vom Begriffsverständnis des Interesses i.S.d. Art. 6 Abs. 1 f) DSGVO erfasst.[26]

Die erste Stufe der Prüfung ergibt somit, dass ein berechtigtes Interesse des Verantwortlichen zum Zeitpunkt der Datenverarbeitung vorliegt.

In der zweiten Stufe ist zu untersuchen, ob die Datenverarbeitung, hier zunächst die Speicherung der Personenstammdaten, zur Verwirklichung des Interesses erforderlich ist.[27] Dies ist dann der Fall, wenn die Verwirklichung nicht mit anderen, milderen Mitteln wie z.B. ohne die Datenverarbeitung oder mithilfe anonymer oder anonymisierter[28] Daten erreicht werden kann.[29] Im vorliegenden Fall ist jedoch die Speicherung und Nutzung der personenbezogenen Daten eine Voraussetzung für die Nutzung der Personalisierungsfunktionen der Gebäudetechnik-Software. Eine andere Möglichkeit steht im derzeitigen Stand der sorgfältig ausgewählten Software und damit mit dem aktuellen Stand der Technik[30] nicht zur Verfügung.

---

[25] *Buchner/Petri*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 146.

[26] *Buchner/Petri*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 146a.

[27] *Buchner/Petri*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 146.

[28] Um anonyme Daten handelt es sich, wenn sie nicht zuvor aus personenbezogenen Daten durch eine entsprechende Verarbeitung anonymisiert werden mussten, d.h. wenn zu keinem Zeitpunkt des Prozesses personenbezogene Daten existieren.

[29] *Schantz*, in: *Simitis*/*Hornung*/*Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG, Art. 6 Abs. 1 DSGVO Rn. 100.

[30] Zur Definition "Stand der Technik" i.S.v. Art. 32 Abs. 1 DSGVO: *Piltz*, in: *Gola* et al., Datenschutz-Grundverordnung VO (EU) 2016/679, Bundesdatenschutzgesetz, Art. 32 DSGVO Rn. 19.

Auch die zweite Stufe des Prüfungsvorgangs ergibt daher, dass die Verarbeitung der Beschäftigten-Stammdaten bis hierher zulässig ist.

In der dritten Stufe der Prüfung schließlich ist zu betrachten, ob möglicherweise die Interessen der betroffenen Personen, hier der Beschäftigten, überwiegen; es muss also eine Abwägung zwischen ihren Interessen und denen des Unternehmens vorgenommen werden.

Auf der Seite der Interessen des Unternehmens sind erstens die wirtschaftlichen Vorteile i.H.v. 3.000,- € p.a. zu nennen, wobei die absolute Größe relativierend in ein Verhältnis zu Umsatz und insbesondere Gewinn des Unternehmens zu setzen ist, was angesichts eines EBIT von rund fünf Millionen € p.a. ihr argumentatives Gewicht verringert. Zweitens trägt die Einsparung der Emissionen durch die Personalisierung der Gebäudetechnik dazu bei, die Umweltziele zu erfüllen. Dieses Kriterium ist nicht nur wichtig für die Außendarstellung des Unternehmens, sondern findet auch Eingang in das Kredit-Scoring der Hausbank der E-GmbH, das wiederum über Vergabe und Konditionen von Darlehen an das Unternehmen mit entscheidet. Das Scoring berührt damit in letzter Konsequenz die unternehmerische Freiheit i.S. d. Art. 16 GRCh.[31] Es besteht daher ein gewichtiges Interesse an der Umsetzung der personalisierten Funktionen.

Auf der Seite der Beschäftigten-Interessen ist zu beleuchten, wie gewichtig die Speicherung von (dienstlicher) E-Mail-Adresse sowie Vor- und Nachnamen datenschutzrechtlich einzuordnen sind. Hier sind zwei Aspekte zu betrachten.

Der erste könnte die Tatsache sein, dass die fraglichen Daten ohnehin bereits mehrfach zulässigerweise gespeichert werden, nämlich in der zentralen Domänenverwaltung, die die Zugangsrechte für die gesamte IT steuert, sowie in der Lohnbuchhaltung des Unternehmens. Allerdings gibt es im aktuellen Stand der wissenschaftlichen Diskussion keinen Hinweis darauf, dass bereits gespeicherte Daten die datenschutzrechtliche Schwelle zur erneuten Speicherung in einem anderen System senken könnten. Vielmehr muss es einen triftigen Grund auch für eine Mehrfachspeicherung geben, es gilt das Prinzip der Datenminimierung gem. Art. 5 Abs. 1 c) DSGVO.[32]

[31] *Buchner/Petri*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 6 Abs. 1 DSGVO Rn. 148.
[32] *Bruns*, in: *Rolfs*, BeckOK Arbeitsrecht, HinSchG § 12, Rn. 20g.

Der zweite Aspekt ist der Schweregrad in den Eingriff der informationellen Selbstbestimmung bei der Speicherung des Namens. Hier ist nicht anzunehmen, dass die Speicherung des Namens oder der allgemein bekannten (dienstlichen) E-Mail-Adresse in einer gesicherten IT-Umgebung für die Zeitdauer des Arbeitsverhältnisses als besonders kritisch einzuschätzen wäre, da beide Daten innerbetrieblich weithin bekannt sind und für sich genommen keine Basis für weitergehende, datenschutzsensible Analytik bieten. Ihre Sensibilität liegt noch unterhalb der von Statusdaten.[33]

Aus diesen Gründen ist davon auszugehen, dass das Interesse des Unternehmens an dieser Stelle überwiegt und die genannten Stammdaten als Grundlage der personalisierten Funktionen gem. Art. 6 Abs. 1 f) DSGVO gespeichert werden dürfen.

bb) Anwesenheitserkennung bestimmter Personen und Speicherung der individuellen Temperatur- und Beleuchtungsprofile

Die Verarbeitung von Anwesenheiten einzelner Personen sowie die Speicherung ihrer individuellen Präferenzen bzgl. Temperatur und Helligkeit könnte gem. Art. 6 Abs. 1 f) zulässig sein.[34]

Dazu müsste es sich bei den erfassten Anwesenheitsdaten um solche mit Personenbezug handeln. Dies ist wegen der Bestimmbarkeit der Person durch die Zuordnung der Anwesenheitserfassung zu ihrem persönlichen Arbeitsplatz gegeben.

Auch hier ist daher die dreistufige Prüfung zur Legitimation der Datenverarbeitung vorzunehmen. Die erste Stufe der Prüfung müsste ergeben, dass ein Interesse des Unternehmens zum Zeitpunkt der Datenverarbeitung vorliegt. Das grundsätzlich bestehende Interesse ist das gleiche wie in Teil 2 C. II. 1. a) aa) hergeleitet. Es besteht fortwährend, also auch zum entscheidenden Zeitpunkt der Speicherung der Komfortwerte sowie zum Zeitpunkt der Anwesenheitserkennung.

Die erste Stufe der Prüfung ergibt somit, dass die Verarbeitung bis hierher nicht zu beanstanden ist.

---

[33] *Kramer*, in: *Weth* et al., Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 188 Rn. 29 - Name und dienstliche E-Mail-Adresse sind in der Aufzählung der Statusdaten nicht erwähnt; sie dürften eher als zentrales Identifikationsmerkmal einzuordnen sein.

[34] Die Anwendung von Art. 22 Abs. 1 DSGVO kommt nicht in Betracht, da das System zwar Personendaten verarbeitet und automatisiert Entscheidungen zu Beleuchtung und Temperierung trifft, diese jedoch keine Rechtswirkung auf die Betroffenen haben, vgl. *Buchner*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 22 DSGVO Rn. 4 ff.

Die zweite Stufe betrifft wiederum die Frage, ob die Datenverarbeitung, hier die Registrierung der Anwesenheit in bestimmten Räumen sowie die Speicherung der Komfortwerte, zur Verwirklichung des Interesses erforderlich ist. Dazu müsste sie nicht anders erreicht werden können. Im vorliegenden Fall ist jedoch die Speicherung und Nutzung der personenbezogenen Daten gerade eine Voraussetzung für die Personalisierung der Funktionen der Gebäudetechnik. Eine andere Möglichkeit steht in der zur Anschaffung geplanten Software nicht zur Verfügung.

Die dritte Stufe der Prüfung erfordert auch an dieser Stelle eine Abwägung aus den Interessen des Unternehmens und denen der Betroffenen.

Bezüglich der Interessen des Unternehmens gelten auch hier die in Teil 2 C. II. 1. a) aa) dargelegten erzielbaren wirtschaftlichen und ideellen Vorteile. Wie im Lösungsansatz (Teil 2 B. I. 2.) erläutert, werden 25% der gesamten Energieersparnis laut der Modellierung des beauftragten Ingenieurbüros allein durch die personalisierten Funktionen erreicht. Die Interessen des Unternehmens sind also als nennenswert zu gewichten.

Dem gegenüber stehen Einwirkungen auf die Interessen der Beschäftigten in Form der Verarbeitung ihrer personenbezogenen Daten. Sobald nämlich zukünftig eine Person an ihrem Schreibtisch arbeitet, soll dies durch die Gebäudesteuerungs-Software registriert und Temperatur sowie Beleuchtung am Arbeitsplatz passend eingestellt werden. Damit könnte also nachvollzogen werden, wer zu welcher Zeit an seinem Schreibtisch sitzt oder nicht. In Verbindung mit dem Bewegungssensor, der die Raumbeleuchtung steuert, ließe sich u.U. auch die Anwesenheit einer bestimmten Person im Raum, also nicht mehr nur am Schreibtisch, ermitteln, je nachdem, ob auch weitere Personen im Raum anwesend sind. Zudem sollen die persönlichen Vorlieben hinsichtlich Beleuchtungsstärke und Temperaturvorlieben gespeichert werden. Dies könnte die Definition des Profilings gem. Art. 4 Abs. 4 DSGVO erfüllen.

Fraglich ist, wie diese Kontroll- und Analysemöglichkeiten hinsichtlich des Beschäftigtendatenschutzes einzuordnen und zu gewichten sind. Bezüglich der Ortungsmöglichkeit einer Person an ihrem Arbeitsplatz in der hier angedachten Art der Umsetzung gibt es allerdings keine konkreten Betrachtungen in der wissenschaftlichen Diskussion. Am ehesten lässt sich die angedachte Technik mit RFID-Systemen vergleichen, die einen am Körper getragenen Transponder detektieren und so den Rückschluss auf den Aufenthalt des Trägers innerhalb ihres

Lesebereiches zulassen. Ebenso wie im hier geplanten Projekt werden also Personen an einzelnen Punkten im Gebäude geortet. Ein solches Szenario wird in der Literatur als zulässig angesehen, wenn die Anwendung unter eine von mehreren Fallgruppen fällt.[35] Die Optimierung von Energieverbräuchen ist jedoch bisher nicht in eine solche eingeordnet worden. Hier sind gedankliche Anleihen bei bekannten Fallgruppen angebracht, die dem Unternehmen finanzielle Vorteile in Form verbesserter Geschäftsprozesse ermöglichen und bei denen eine Zulässigkeit der Verarbeitung personenbezogener Daten als zulässig betrachtet wird.[36] Werden also im vorliegenden Fall die verarbeiteten Daten ausschließlich zu Zwecken der Senkung des Energieverbrauches verarbeitet und zudem Art. 25 Abs. 2 S. 2 DSGVO entsprechend nicht unnötig lange aufbewahrt, dürfte die Beeinträchtigung der Interessen der Beschäftigten so gering sein, dass die Interessen des Unternehmens überwiegen. Diese Bedingungen sind erfüllt, da die Daten der Anwesenheitserfassung am Arbeitsplatz ausschließlich vom Smart-Building-Server zu Steuerungszwecken verarbeitet und umgehend automatisch gelöscht werden, wenn sie zum Aktivieren der aktuell gewünschten Klima- und Lichteinstellungen nicht mehr benötigt werden.

Zu untersuchen ist weiterhin, ob das Profiling i.S.v. Art. 4 Abs. 4 DSGVO eine separat zu betrachtende Auswirkung auf die Interessenslage der Beschäftigten hat. Dazu müsste es besonderen Regularien unterworfen sein. Tatsächlich sieht die DSGVO in Art. 22 bereits in ihrer Überschrift eine besondere Behandlung des Profilings vor. Allerdings kombiniert sie es terminologisch mit darauf basierenden automatisierten Einzelfallentscheidungen. Dies wird in der Literatur teils kritisch gesehen, da der vorbereitende Prozess der Datensammlung und die nachfolgend automatisch ablaufende Entscheidung separat zu betrachten seien und die terminologische Zusammenfassung unscharf sei.[37] Im Ergebnis ist die h.M., dass Profiling nur im Zusammenhang mit automatisierten Einzelfallentscheidungen, die für den betroffenen rechtliche Wirkung entfalten, aus datenschutzrechtlicher Sicht einer besonderen Betrachtung bedarf, während das reine Profiling unter die allgemeinen rechtlichen Regeln der Datenverarbeitung fällt.[38] Teils wird sogar die Auffassung

[35] *König*, Beschäftigtendatenschutz in der Beratungspraxis, § 5 Rn. 87 ff.
[36] *Byers*, in: *Weth* et al., Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 470 Rn. 29.
[37] *Buchner*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 22 Rn. 4.
[38] EG 72 DSGVO; *von Lewinski*, in: *Wolff*/*Brink*, Datenschutzrecht, Bereichsspezifischer Datenschutz, DS-GVO, BDSG, Art. 22 DSGVO Rn. 1 ff; *Martini*, in: *Paal*/*Pauly*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 22 DSGVO Rn. 2; *Scholz*, in: *Simitis*/*Hornung*/*Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG, Art. 22 DSGVO Rn. 5.

vertreten, es handele sich bei der Sammlung von Daten zu persönlichen Vorlieben (im vorliegenden Fall zu Temperatur und Helligkeit am Arbeitsplatz) erst dann um Profiling, wenn diese Daten auch bewertet und analysiert sowie zu weiteren Zwecken der Vorhersage ausgewertet werden.[39] Im Ergebnis ist also die Speicherung der persönlichen Temperatur- und Beleuchtungspräferenzen der Beschäftigten, selbst wenn es sich um Profiling handelt, rechtlich nicht anders zu bewerten als die Speicherung anderer personenbezogener Daten.

Die Erfassung der Anwesenheit am Arbeitsplatz sowie die Speicherung und Auswertung der bevorzugten Arbeitstemperatur und -Helligkeit ist somit gem. Art. 6 Abs. 1 f) DSGVO zulässig.

cc) Kamerabasierte Personen-Zustandserkennung in gemeinschaftlich genutzten Räumen

Fraglich ist, ob die Speicherung der Bilder der von der Kamera erfassten Personen sowie ihre fallweise Weiterleitung an ein externes Unternehmen zum Zweck des optimalen Energiemanagements zulässig ist.

In Frage kommen Art. 9 Abs. 2 b) DSGVO , §4 Abs. 1 Nr. 3 BDSG oder Art. 6 Abs. 1 f) DSGVO als Rechtsgrundlage.

Die Anwendbarkeit von Art. 9 Abs. 2 b) DSGVO setzt voraus, dass biometrische Daten der erfassten Personen verarbeitet werden. Aufgezeichnet werden beim geplanten Auswertungsvorgang auch die Gesichter der Beschäftigten, diese sind grundsätzlich geeignet, eine Person eindeutig zu identifizieren und könnten als biometrisches Merkmal gelten. Allerdings müssten die Gesichtsdaten nach dem Wortlaut der Verbotsnorm Art. 9 Abs. 1 DSGVO („zur eindeutigen Identifizierung einer natürlichen Person“) auch zu diesem Zweck verarbeitet werden und, damit das System zur Erkennung funktioniert, auch mit zuvor gespeicherten Gesichtsdaten abgeglichen werden.[40] Diese Funktionalität ist im beschriebenen Fall weder implementiert noch geplant. Da Art. 9 Abs. 1 DSGVO aus diesem Grund nicht greift, kann auch Art. 9 Abs. 2 b) DSGVO nicht angewendet werden.

Zu Anwendbarkeit von §4 Abs. 1 Nr. 3 BDSG ist fraglich, ob die auszustattenden Räume, also die Kantine und der Mehrzweckraum, unter die Definition „öffentlich

[39] *Scholz*, in: *Simitis*/*Hornung*/*Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG, Art. 4 Nr. 4 DSGVO Rn. 1 ff.
[40] *Byers/Winkler/Stelter*, NZA 2023, 457 (458).

zugänglicher Räume“ i.S.d. Norm fallen. Beide Räume sind zwischen 7 und 17 Uhr durch die Hauteingangstür und jeweils zwei weitere, nicht verschlossene Türen für jedermann, also für die Öffentlichkeit, zugänglich.

Jedoch ist die Vorschrift anders auszulegen. Entscheidend ist, ob die fraglichen Bereiche dem öffentlichen Verkehr auch gewidmet sind.[41] Sofern der Wille, dass der Zutritt zum Bürogebäude nicht jedem offensteht, „nach außen deutlich erkennbar“ ist, gilt es nicht als öffentlich i.S.d. Norm. Dies ist der Fall, da an der Eingangstür ein markantes Schild mit dem Text „Zutritt nur für Betriebsangehörige“ angebracht ist. Damit fallen die beiden fraglichen Räume nicht unter die Definition von §4 Abs. 1 Nr. 3 BDSG.

Für die Prüfung eines Erlaubnistatbestandes gem. Art. 6 Abs. 1 f) DSGVO greift wiederum die dreistufige Prüfung.[42]

Die erste Stufe betrifft das Interesse des Unternehmens an der Maßnahme zum Zeitpunkt der Datenverarbeitung. Dieses Interesse besteht in der Verbesserung der Erkennungsergebnisse. Zwar hat die Übertragung der Bilder keine direkte Auswirkung auf die Senkung des Energieverbrauches – diese ist eigentliches Primärziel der geplanten Maßnahme –, jedoch ist ein auf Künstlicher Intelligenz basierendes System auf Input zum Lernen angewiesen, um die Qualität der Algorithmen stetig zu verbessern.[43] Über diese Qualitätsverbesserung würde das geplante System langfristig immer effektiver arbeiten, wodurch der Energiebedarf in den betroffenen Räumlichkeiten sänke.

Die erste Stufe der Prüfung ergibt also, dass zum Zeitpunkt der Datenverarbeitung ein berechtigtes Interesse des Unternehmens vorliegt.

Die zweite Stufe betrifft die Prüfung, ob die Datenverarbeitung, in diesem Fall die Speicherung und Weiterleitung der Bilder, zur Verwirklichung des Interesses erforderlich ist. Dazu müsste sie wiederum nicht anderweitig umsetzbar sein. Dies ist der Fall, denn die Verbesserung der KI-Erkennungsleistung lässt sich nur durch Zuführung von aufbereitetem Lernmaterial, hier die manuell eingeordneten Videosequenzen, erreichen.

[41] *Starnecker*, in: *Gola* et al., Datenschutz-Grundverordnung VO (EU) 2016/679, Bundesdatenschutzgesetz, BDSG § 4 Rn. 25.
[42] *Buchner/Petri*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 146.
[43] *Groh*, in: *Weber*, Rechtswörterbuch, "Künstliche Intelligenz".

Auch die zweite Stufe der Prüfung ergibt somit, dass bis hierher die Verarbeitung der Videodaten zulässig ist.

In der dritten Stufe sind die Interessen des Unternehmens gegen die der Beschäftigten abzuwägen.

Auf Seiten der Interessen des Unternehmens ist zu berücksichtigen, dass nach wie vor die in Teil 2 C. II. 1. a) aa) hergeleitete Kombination aus wirtschaftlichen und ideellen Interessen gilt. Jedoch ist die Wirkung und somit die Gewichtbarkeit der Maßnahme weitaus geringer einzuordnen, da es sich lediglich um eine Optimierungsmaßnahme zweier (wenn auch großer) Räume mit einem Bruchteil der Wirkung des Gesamtprojektes handelt. Die Gewichtung der Interessen des Unternehmens ist somit als gering einzuordnen.

Auf der Seite der Interesse der Betroffenen hingegen könnte die Verarbeitung von Videoseqenzen, die sie betreffen, ein erheblicher Eingriff in ihre Grundrechte bedeuten. Allerdings könnte es eine Rolle spielen, dass hier keine Videoüberwachung im herkömmlichen Sinne stattfindet. Das Material wird nicht zur Verhaltens- oder Leistungskontrolle verwertet, sondern lediglich zur Optimierung von KI-Algorithmen. Nach der Definition des BAG[44] ist die Definition einer „Videoüberwachungsanlage“ also nicht erfüllt. Darauf kommt es jedoch nach Ansicht des Bundesverfassungsgerichtes[45] nicht an. Es begründet seine Entscheidung mit dem allgemein geltenden Recht auf informationelle Selbstbestimmung. Übertragen auf den vorliegenden Fall bedeutet dies, dass der Verwendungszweck der Aufnahmen nicht die Gewichtung der Betroffenen-Interessen verringern darf.

Einem als geringwertig einzuschätzenden Interesse des Unternehmens treten also gewichtige Interessen der Beschäftigten gegenüber. Die Datenverarbeitung ist mangels eines Erlaubnistatbestandes aus Art. 6 Abs. 1 DSGVO nicht rechtmäßig.

Aus diesem Grund kann die Prüfung der Übertragung der Daten nach Asien, deren Rechtmäßigkeit anhand Art. 45 Abs. 1 DSGVO zu untersuchen wäre, entfallen.

[44] BAG, Beschl. vom 29.06.2004 - 1 ABR 21/03, NJW 2005, 313.
[45] BVerfG, 1. Kammer des 1. Senats, Beschl. vom 23.02.2007 - 1 BvR 2368/06, NVwZ 2007, 688 (690).

b) Smart Building - Mitbestimmungsrecht des Betriebsrates gem. § 87 Abs. 1 Nr. 6 BetrVG

Der Betriebsrat könnte beim Betrieb des Smart-Building-Systems ein Mitspracherecht gem. § 87 Abs. 1 Nr. 6 BetrVG haben.

Dazu müsste es sich bei dem System, bestehend aus der im Gebäude installierten Sensorik und dem Server mit den Steuerungsfunktionen, um eine Vorrichtung handeln, die dazu bestimmt ist, das Verhalten oder die Leistung der Beschäftigten zu überwachen.

Fraglich ist zunächst, ob die gesetzliche Definition der „Überwachung" im vorliegenden Fall zutrifft. Die in der Funktionsbeschreibung vorgesehene automatisierte Feststellung, wer zu welcher Zeit an seinem Schreibtisch sitzt, könnte bereits als Überwachung i.S.d. Norm zu verstehen sein. Tatsächlich wird der Begriff der Überwachung restriktiv ausgelegt[46], so dass bereits diese Funktion ein Mitspracherecht des Betriebsrates auslösen könnte.

Dazu müsste weiterhin die An- und Abwesenheit der einzelnen Beschäftigten an ihren Schreibtischen als „Verhalten" i.S.d. Norm gelten. Auch dies ist der Fall; jedes „Tun oder Unterlassen" gilt als „Verhalten" i.S.d. Norm.[47]

Zusätzlich müsste die Funktion aber auch zur Überwachung „bestimmt" sein. Dies ist nicht der Fall; der Arbeitgeber hat die Einrichtung geplant, um seinen Energieverbrauch zu optimieren. Das System ist in keiner Weise auf eine Art von Verhaltens- oder Leistungskontrolle in der Form ausgelegt, dass Beschäftigte bzgl. ihrer Arbeitsleistung oder ihres Verhaltens kontrolliert oder überwacht werden sollen. Darauf kommt es allerdings nicht an. Die Rechtsprechung hat nämlich durch Auslegung der Norm das Mitbestimmungsrecht von der Kontrollabsicht des Arbeitgebers entkoppelt; es reicht bereits die Eignung der technischen Vorrichtung zur Kontrolle aus.[48] Im Folgenden wird daher ausschließlich die Eignung der geplanten Funktionen zur Überwachung von Verhalten oder Leistung der Beschäftigten als Voraussetzung für ein Mitbestimmungsrecht geprüft, nicht aber eine mögliche Absicht hierzu.

Eine Eignung zur Kontrolle zumindest des Verhaltens, in Teilen möglicherweise auch der Arbeitsleistung, würde das System funktional durchaus ermöglichen. Die

[46] *Clemenz*, in: *Henssler*/*Willemsen*/*Kalb*, Arbeitsrecht, § 87 BetrVG Rn. 118.
[47] *Clemenz*, in: *Henssler*/*Willemsen*/*Kalb*, Arbeitsrecht, § 87 BetrVG Rn. 119.
[48] *Kramer*, in: *Weth* et al., Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 184 Rn. 16.

Auswertung der Anwesenheit bzw. Nicht-Anwesenheit am Schreibtisch ließe diverse Rückschlüsse auf das Arbeits- und Pausenverhalten z.B. bei Rauchern oder bei solchen Beschäftigten zu, die einen überdurchschnittlichen Hang zum Ausleben sozialer Kontakte innerhalb der Arbeitszeit besitzen.

Bei der Einführung des Smart-Building-Systems besteht somit bereits durch die Anwesenheitserfassung am Schreibtisch ein Mitspracherecht des Betriebsrates gem. § 87 Abs. 1 Nr. 6 BetrVG.

2. Fall 2 – Ortung von Beschäftigten

a) Mögliche Erlaubnistatbestände aus Art. 6 Abs. 1 b) Alt. 1, c), d), f) DSGVO

aa) Ortung von Beschäftigten im Gefahrenbereich des Kranlagers

Die Ortung von Beschäftigten im Gefahrenbereich des Kranlagers könnte gem. Art. 6 b), d) oder f) DSGVO zulässig sein.

Die Ortung könnte gem. Art. 6 b) Alt. 1 DSGVO zulässig sein. Dazu müsste sie zur Durchführung eines Vertragsverhältnisses, hier des Arbeitsvertrages zwischen den Beschäftigten und der M AG, erforderlich sein. Allerdings sind Maßnahmen zum Arbeitsschutz nicht direkt zur Durchführung des Vertragsverhältnisses erforderlich. Sie sind eine vertragliche Nebenpflicht, die sich allgemein aus § 618 Abs. 1 BGB, § 62 HGB, § 3 Abs. 1 Arbeitsschutzgesetz (ArbSchG) und ggf. weiteren speziellen Vorschriften ergibt. Fraglich ist also, ob die Norm neben dem Inhalt des Hauptvertrages auch dessen Nebenpflichten adressiert. Dies wird in der Literatur bejaht.[49]

Zusätzlich wäre es nötig, dass trotz einer durch den EuGH geforderten restriktiven Auslegung[50] der Erforderlichkeit die Datenverarbeitung gegeben ist. Erforderlich ist eine Verarbeitung personenbezogener Daten dann, wenn der beabsichtigte Zweck nicht mit milderen Mitteln umsetzbar ist.[51] Fraglich ist also hier, ob es eine Alternative zur Ortung gäbe. Dies ist zu verneinen, da zuvor alle Alternativen wie

[49] *Buchner/Petri*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 32; *Schantz*, in: *Simitis*/*Hornung*/*Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG, Art. 6 Abs. 1 DSGVO Rn. 24; *Albers/Veit*, in: *Wolff*/*Brink*, Datenschutzrecht, Bereichsspezifischer Datenschutz, DS-GVO, BDSG, Art. 6 DSGVO Rn. 43.

[50] EuGH, 04.07.2023 – C-252/21, ECLI:EU:2023:537.

[51] *Schantz*, in: *Simitis*/*Hornung*/*Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG, Art. 6 Abs. 1 DSGVO Rn. 100.

eine Video-Überwachung des Gefahrenbereiches geprüft und für nicht umsetzbar befunden wurden.

Auch die Genauigkeit der Ortung könnte ein Entscheidungskriterium sein. Wie beschrieben, misst die verwendete AOA-Technologie den Aufenthaltsort einer Person sehr präzise und mit hoher Erfassungsfrequenz. In der Rechtsliteratur kommt sie bislang nicht vor; die genaueste erwähnte Indoor-Technologie ist RFID[52], die jedoch nur eine Genauigkeit in der Größe des Radius‘ des Erfassungsbereiches der RFID-Lesevorrichtung ermöglicht. Eine derart engmaschige und zugleich flächendeckende Ortung von Personen wie im vorliegenden Fall wäre jedoch damit nicht möglich.[53] Daraus ergibt sich die Frage, ob die Genauigkeit der AOA-Technologie Konsequenzen auf die datenschutzrechtliche Bewertung hat. Wäre dies der Fall, müssten die in der Literatur angestellten Überlegungen zur Zulässigkeit der Ortung mithilfe einer ungenauen Technologie nochmals kritischer bewertet werden. Hilfreich ist hier ein Vergleich mit Überlegungen zur GPS-Ortung von Beschäftigten. Eine solche wird unter bestimmten Voraussetzungen als erforderlich angesehen. Sie muss aber beschränkt sein auf den erforderlichen Einsatzzweck und -zeitpunkt; die Bildung vollständiger, engmaschiger Bewegungsprofile fällt in aller Regel nicht unter eine solche Erforderlichkeit und gilt nur in bestimmten Situationen, die z.B. die Sicherheit von Beschäftigten betreffen, als erforderlich.[54]

Aus diesen Ansichten zur GPS-Ortung lässt sich also ableiten, dass der Betrieb eines Ortungssystems bzgl. seiner Erforderlichkeit aus datenschutzrechtlicher Sicht umso kritischer zu betrachten ist, je höher seine Genauigkeit in örtlicher und zeitlicher Hinsicht ist. Das geplante System zeichnet den Standort im Abstand weniger Sekunden mit einer Genauigkeit von unter 50 cm auf. Insofern sind die verarbeiteten Daten aus datenschutzrechtlicher Sicht äußerst sensibel. Andererseits ist diese Präzision im Kranlager auch erforderlich, da der Kran den lokalisierten Ort umfahren soll und der genaue Aufenthaltsort der Person dazu zu jedem Zeitpunkt bekannt

[52] *Thüsing/Forst*, in: *Thüsing*, Beschäftigtendatenschutz und Compliance, §12 Rn. 7 ff; *Riesenhuber*, in: *Wolff/Brink*, Datenschutzrecht, Bereichsspezifischer Datenschutz, DS-GVO, BDSG, § 26 BDSG Rn. 163; *Riesenhuber*, in: *Brink/Wolff/v. Ungern-Sternberg*, BeckOK Datenschutzrecht, § 26 BDSG Rn. 163; *Byers*, in: *Weth* et al., Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 464 Rn. 7,8.

[53] In den vorgenannten Quellen werden auch Wearables und Datenbrillen als Ortungs-Hardware erwähnt, ohne dabei jedoch auf die verwendete Technologie einzugehen. Es sind daher keine Annahmen zur erzielbaren Genauigkeit möglich.

[54] *Seifert*, in: *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG, Art. 88 DSGVO Rn. 141.

sein muss. Eine laufende, sehr genaue Ortung im Bewegungsbereich des Krans ist damit zulässig.

Fraglich ist jedoch, ob die Ortungsdaten, wenn die betroffene Person das Kranlager wieder verlassen hat, nach dem Ortungsereignis und der Beseitigung der Gefahrensituation noch gespeichert werden müssen. Wie im Lösungsansatz beschrieben, werden die Daten nämlich erst gelöscht, wenn der Datenträger des Servers weitgehend gefüllt ist. Gefährdungstechnisch ist dies jedenfalls nicht erforderlich; sobald eine Person das Kranlager wieder verlassen hat, könnten die historischen Datensätze im Interesse der Datenminimierung gelöscht werden, da keine Gefahr mehr besteht und die Erforderlichkeit der Datenverarbeitung entfallen ist.[55] Allerdings steht dem entgegen, dass die Personen, die sich im Kranlager aufhalten, dabei oftmals entgegen den Anweisungen im Sicherheitshandbuch der Firma handeln. Dort sind Verhaltens- und Kommunikationsregeln festgelegt, die auch Bedingungen und Verhaltensvorschriften zum Aufenthalt in dieser Gefahrenzone regeln. Die Speicherung der personenbezogenen Daten ist also auch nach dem sicherheitsrelevanten Ereignis erforderlich, um ggf. eine individuelle Sicherheitsnachschulung planen zu können. Ist diese allerdings erfolgt, entfällt auch die Erforderlichkeit und die Daten müssten gelöscht werden.[56] Eine solche ereignisbezogene Löschung ist im geplanten Konzept nicht vorgesehen, die Speicherfrist bemisst sich stattdessen nach der Datenträgergröße.

Grundsätzlich ist also zwar von der Erforderlichkeit einer exakten und zeitgenauen Ortung der Personen sowie der nachfolgenden Speicherung der Ortungsdaten im Gefahrenbereich auszugehen. Allerdings müsste die Speicherfrist der Daten so verkürzt werden, dass nach erfolgter Entscheidung über eine Sicherheitsschulung der betroffenen Beschäftigten die Daten gelöscht werden.

Art. 6 Abs. 1 b) Alt. 1 DSGVO wäre also eine mögliche Rechtsgrundlage für den Betrieb des Ortungssystems mit der Einschränkung, dass die Speicherfrist der Ortungsdaten auf das notwendige Maß verkürzt wird.

Auch eine Berufung auf Art. 6 Abs. 1 d) DSGVO wäre möglicherweise statthaft. Dazu müssten durch den Betrieb des Systems lebenswichtige Interessen der

[55] Zur Datenminimierung allgemein: *Pötters*, in: *Gola* et al., Datenschutz-Grundverordnung VO (EU) 2016/679, Bundesdatenschutzgesetz, Art. 5 DSGVO Rn. 22.

[56] *Schantz*, in: *Brink*/*Wolff*/*v. Ungern-Sternberg*, BeckOK Datenschutzrecht, Art. 5 DSGVO Rn. 32 f; *Worms*, in: *Brink*/*Wolff*/*v. Ungern-Sternberg*, BeckOK Datenschutzrecht, Art. 17 DSGVO Rn. 25 f.

betroffenen Person, hier der Beschäftigten, geschützt werden. Tatsächlich dient das System u.a. dazu, den Aufenthalt einer Person im Gefahrenbereich des Krans festzustellen und schützende Maßnahmen einzuleiten. Insoweit wäre die Vorschrift einschlägig. Eine weitere Voraussetzung für ihre Anwendbarkeit ist, dass die betroffene Person nicht imstande ist, ihre Einwilligung zur Verarbeitung der Daten zu geben.[57] Im vorliegenden Fall ist jedoch die Verarbeitung der personenbezogenen Daten gerade die Voraussetzung dafür, die Gefahr festzustellen, in der die betroffene Person möglicherweise schwebt. Die Verarbeitung hat also zum Zeitpunkt des Gefahreneintrittes bereits stattgefunden. Dies schränkt die Anwendbarkeit der Norm ein, da sie offensichtlich andere Lebenssituationen adressiert. Zudem ist eine Ortung einer Person nicht immer mit akuter Gefahr verbunden. So würden auch dann laufend Ortungen durchgeführt, wenn der Kran im Wartungsmodus ist und keinerlei Bedrohung für Leib und Leben darstellt. Ebenso kann sich im weitläufigen Lager an vollkommen anderer Stelle arbeiten, als die geortete Person sich in gerade befindet, so dass in dem Moment keine akute Gefahr für Leib und Leben von ihm ausgeht. Die Vorschrift wäre also zumindest nicht durchgängig anwendbar, so dass sie keine ständige Rechtsgrundlage für den Betrieb des Systems im Kranlager bilden könnte. Zudem ist sie subsidiär und wäre nur anzuwenden, wenn nicht eine andere Norm einschlägig wäre.[58]

Die Berufung auf Art. 6 Abs. 1 d) ist daher nicht möglich.

Möglicherweise könnte noch Art. 6 Abs. 1 f) DSGVO eine rechtliche Basis für die ständige Ortung von Personen im Kranlager darstellen. Die Anwendbarkeit dieser Norm ist auch hier im Rahmen der dreistufigen Prüfung[59] vorzunehmen.

In der ersten Prüfungsstufe ist das berechtigte Interesse des Verantwortlichen oder eines Dritten zu untersuchen. Dieses könnte in mehreren Bereichen bestehen.[60] Zunächst kommt das Interesse an der Verhinderung von Arbeitsunfällen in Frage. Dieses Interesse wiederum kann wiederum mehrschichtig sein. Zunächst sind ethisch-ideelle Aspekte denkbar. Dazu müssten in der M-GmbH entsprechende Selbstverpflichtungen oder zumindest ein entsprechender ethischer Konsens bestehen. Dies

[57] *Schulz*, in: *Gola* et al., Datenschutz-Grundverordnung VO (EU) 2016/679, Bundesdatenschutzgesetz, Art. 6 DSGVO Rn. 49.
[58] *Roßnagel*, in: *Simitis*/*Hornung*/*Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG, Art. 6 Abs. 1 DSGVO Rn. 62.
[59] *Buchner/Petri*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 146.
[60] *Robrahn/Bremert*, ZD, 2018, S. 291, 292.

ist der Fall; die Firma hat bereits vor langer Zeit in ihren Grundsätzen der Unternehmensethik schriftlich u.a. die laufende Verbesserung der Arbeitssicherheit als Aspekt der Beschäftigtenfürsorge definiert.

Weiterhin kann sich die M-GmbH auf ein finanzielles Interesse zur Verhinderung von Arbeitsunfällen berufen, da jedes Ereignis dieser Art kurzfristige Kosten im Rahmen der Lohnfortzahlung im Krankheitsfall und Prozesskosten für die Disposition von Ersatzpersonal wie auch langfristige Aufwendungen für erhöhte Versicherungsbeiträge verursacht.

Schließlich sind gem. dem Wortlaut der Norm auch Drittinteressen zu berücksichtigen. Diese manifestieren sich in Behandlungs- oder gar Verrentungskosten, die die Sozialversicherungsträger nach einem Arbeitsunfall zahlen müssten. Schließlich hat auch die gesamte Volkswirtschaft ein Interesse an der Vermeidung von Arbeitsunfähigkeiten, da diese einen Verlust an Wertschöpfung und stattdessen einen Werteverzehr mit sich bringen.[61]

Die erste Stufe der Prüfung zeigt somit ein fortwährendes berechtigtes Interesse seitens der M AG und Dritter.

In der zweiten Stufe ist die Erforderlichkeit der Datenverarbeitung, also der Erfassung und Speicherung der Ortungsdaten, zu prüfen. Diese Prüfung ist bereits im Rahmen der Betrachtungen zu Art. 6 Abs. 1 b) Alt. 1 DSGVO erfolgt. Sie ist gegeben unter der Voraussetzung, dass eine Reduktion der Speicherdauer der Ortungsdaten durchgeführt wird.

Doch selbst wenn diese Anpassung erfolgt wäre, müsste in der dritten Prüfungsstufe eine Abwägung der Interessen der M AG als Verantwortlicher und der Betroffenen zugunsten des Arbeitgebers ausfallen.

Auf der Seite der Interessen der M AG als Verantwortlicher steht das Interesse, Arbeitsunfälle zu vermeiden und mit den optionalen Sicherheitsschulungen ein Instrument zu nutzen, die Arbeitssicherheit gemäß der eigenen Statuten konstant zu verbessern. Zudem besteht ihr Interesse darin, sich nicht durch mangelnde Erfüllung ihrer Fürsorgepflichten, die allgemein aus § 242 Abs. 2 BGB[62] und ggf. aus weiteren Spezialvorschriften des Arbeitsschutzes hervorgehen, in eine rechtlich

[61] Im Jahr 2022 betrug der geschätzte Verlust an Bruttowertschöpfung durch Arbeitsunfälle 207 Mrd. € (https://www.baua.de/DE/Themen/Monitoring-Evaluation/Zahlen-Daten-Fakten/Kosten-der-Arbeitsunfaehigkeit.html, abgerufen am 05.03.2024)

[62] *Spinner*, in: *Säcker* et al., MüKoBGB, § 611a BGB Rn. 901 f.

nachteilige Position zu begeben.[63] Diese Interessen sind hoch zu gewichten, da die rechtlichen Nachteile und ihre Folgen sich, je nach Anzahl und Schwere der potenziellen Arbeitsunfälle, erheblich auf den Fortbestand der Firma auswirken können.

Auf der Seite der Beschäftigteninteressen greift, wie bereits im Abschnitt der Erforderlichkeitsprüfung ausgeführt, eine engmaschige Ortung innerhalb des Kranlagers erheblich in das Persönlichkeitsrecht der Beschäftigten ein. Fraglich ist, ob die präzise Echtzeitortung der dort arbeitenden Personen sogar eine verbotene Totalüberwachung darstellt.[64] Dem ist allerdings zu entgegnen, dass der Wortanteil „Total" sich nicht nur auf einen örtlich begrenzten Bereich, hier das Kranlager, beziehen kann, sondern den Beschäftigten während seiner gesamten beruflichen Tätigkeit betreffen müsste. Bezüglich der Ortung im Kranlager ist dies nicht der Fall, es handelt sich um einen örtlich begrenzten Bereich, der nur gelegentlich betreten wird. Zudem fehlen bei der Ortung Merkmale, die bei anderen Überwachungsmaßnahmen die Intensität des Grundrechtseingriffes wesentlich prägen[65], z.B. bei einer Videoüberwachung die jederzeitige Auswertungsmöglichkeit der Leistung, der Gestik und Mimik etc.[66] Der Eingriff in die Interessen der Beschäftigten ist somit zwar wesentlich, jedoch örtlich und zeitlich begrenzt und weniger intensiv als bei einer Videoüberwachung des gleichen Bereiches.

Die Interessensabwägung ist hier also angesichts der potenziell existenzentscheidenden Interessen des Verantwortlichen und der maßvollen Eingriffe in die Interessen der Betroffenen zugunsten der M AG zu entscheiden.

Das Ortungssystem im Kranlager kann somit gestützt auf Art. 6 Abs. 1 f) DSGVO betrieben werden, jedoch unter der erläuterten Maßgabe, dass die Speicherfrist entsprechend den Ausführungen in der Erforderlichkeitsprüfung verkürzt wird.

Sowohl Art. 6 Abs.1 b) als auch f) DSGVO können eine Rechtsgrundlage für den Betrieb des Ortungssystems im Kranlager darstellen, sofern die Daten nach einer Änderung am Konzept nur so lange gespeichert werden, wie dies erforderlich ist.

[63] *Spinner*, in: *Säcker* et al., MüKoBGB, § 611a Rn. 906.
[64] *Schmidl*, in: *Hauschka*/*Moosmayer*/*Lösler,* Corporate Compliance, § 28 Rn. 367 f.
[65] *Thüsing/Forst*, in: *Thüsing*, Beschäftigtendatenschutz und Compliance, § 12 Rn. 28.
[66] Zu den Merkmalen eines schwerwiegenden Eingriffes in das Persönlichkeitsrecht: BAG, Beschl. vom 29.06.2004 - 1 ABR 21/03, NJW 2005, 313.

bb) Ortung von Beschäftigten im Produktionsbereich

Der Betrieb des Ortungssystems im Produktionsbereich könnte gem. Art. 6 Abs. 1 b) Alt. 1 oder f) DSGVO rechtmäßig sein.

Mit einem auf Art. 6 Abs. 1 b) Alt. 1 DSGVO gestützten Betrieb des Systems müsste die M AG eine rechtliche Verpflichtung aus den Arbeitsverträgen mit den Beschäftigten erfüllen. Wie im vorstehenden Abschnitt aa) erläutert, kann dies auch eine vertragliche Nebenpflicht sein. In Frage käme hier die Fürsorge in Form einer schnellen Auffindbarkeit bei Betriebsunfällen, bei denen Personen hilflos sind und sich nicht aus eigener Kraft in Sicherheit bringen können. Die Schwere der Unfallfolgen würde sich dadurch erfahrungsgemäß verringern. Die M AG würde mit dem Betrieb des Ortungssystems also eine rechtliche Nebenpflicht aus den Arbeitsverträgen erfüllen.

Zusätzlich müsste die Verarbeitung der Daten aber auch erforderlich, also der beabsichtigte Zweck nicht mit milderen Mitteln zu erreichen sein.[67] Hieraus ergibt sich angesichts der geplanten dauerhaften Lokalisierung der Beschäftigten die Frage, ob zur Abmilderung der Folgen eines Ereignisses, das nur selten auftritt, eine jahrelange Echtzeit-Ermittlung der Ortungsdaten im Produktionsbereich erforderlich ist. Es liegt auf der Hand, dass dies im Sinne von Art. 5 Abs. 1 c) DSGVO zu verneinen ist.[68] Möglicherweise zulässig dagegen wäre eine Ortung dann, wenn sie nur im Fall der notwendigen Rettung hilfloser Personen aktiviert würde.[69] Bei einem Szenario wie im beschriebenen Vorfall gäbe es kein milderes Mittel zur schnellen Rettung, da aufgrund der u.U. schlechten Sichtbedingungen keine vergleichbar zügige visuelle Ortung durch Bergungskräfte möglich ist.

Art. 6 Abs. 1 b) Alt. 1 DSGVO wäre also dann als Rechtsgrundlage geeignet, wenn eine Ortung der Beschäftigten nur im Unglücksfall durchgeführt wurde. Da dies im vorgestellten Konzept nicht der Fall ist, kann der Betrieb des Systems nicht ohne Modifikationen auf Grundlage dieser Norm geschehen.

---

[67] *Schantz*, in: *Simitis*/*Hornung*/*Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG, Art. 6 Abs. 1 DSGVO Rn. 100.

[68] so auch *Weichert*, NZA 2017, 565 (567).

[69] In diesem Fall käme auch die Anwendung v. Art. 6 Abs. 1 d) DSGVO in Betracht. Diese Norm soll jedoch aufgrund ihrer Subsidiarität nur herangezogen werden, wenn sich die Anwendung des Systems nicht auf andere Rechtsgrundlagen stützen lässt (EG 46 S. 2 DSGVO).

Eine weitere denkbare Rechtsgrundlage ist Art. 6 Abs. 1 f) DSGVO. Auch in diesem Fall ist wiederum eine Prüfung der Einschlägigkeit in drei Schritten durchzuführen.[70]

Der erste Schritt betrifft das berechtigte Interesse der M AG zum Zeitpunkt der Verarbeitung der Daten, also des Ortungsvorganges. Hier ist zu unterscheiden zwischen dem normalen Geschäftsbetrieb im Unternehmen und dem Ausnahmefall der notwendigen Evakuierung.

Im Fall der Evakuierung besteht ein mehrschichtiges Interesse des Unternehmens an einer Ortung der zu evakuierenden Beschäftigten. Dieses beginnt bei der ethisch geprägten Selbstverpflichtung, Maßnahmen zur Erhaltung die Gesundheit der Mitarbeitenden zu treffen, also auch nachteilige Folgen von Ausnahmeereignissen zu minimieren. Es handelt sich also dabei um ein ideelles Interesse. Zudem kommen auch berechtigte wirtschaftliche Interessen in Frage, so z.B. die Verringerung der Folgekosten von Personalausfällen oder auch eine effiziente Brandbekämpfung, die erst nach Evakuierung aller gefährdeten Personen eingeleitet werden kann und die den Schadensumfang umso geringer hält, je früher sie begonnen wird. Die Interessen ähneln somit denen aus dem vorstehenden Abschnitt aa) („Ortung im Kranlager"), beziehen sich aber auf eine konkrete, bereits eingetretene Situation und nicht auf eine nur potenzielle Gefahr für die Beschäftigten.

Im Fall des Normalbetriebes dagegen besteht kein erkennbares berechtigtes Interesse der M AG an der Ortung der Beschäftigten. Zwar würden sich die erhobenen Daten auch für Zwecke eignen, die sich ein wirtschaftliches Interesse stützen ließen, z.B. die Leistungskontrolle von Beschäftigten oder die Optimierung logistischer Prozesse, jedoch ist diese Funktionalität nicht vorgesehen. Vielmehr nähert man sich bei der lückenlosen Echtzeitortung einer Totalüberwachung an, da bei der Teilfunktion „Ortung im Produktionsbereich" eine dauerhafte, anlasslose Aufzeichnung der Aufenthaltsorte und Laufwege aller Beschäftigten stattfindet.

Ein berechtigtes Interesse der M AG kann somit nur im Fall des akuten Bedarfes bei einer Evakuierungssituation angenommen werden.

Die zweite Prüfungsstufe, die sich auf die Erforderlichkeit der geplanten Maßnahme bezieht, kann aus den Betrachtungen zur Einschlägigkeit von Art. 6 Abs. 1

[70] *Buchner/Petri*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 6 DSGVO Rn. 146.

b) Alt. 1 DSGVO übernommen werden. Im Ergebnis ist die Ortung auch hier erforderlich, wenn ein Evakuierungsfall eintritt, nicht jedoch im Normalbetrieb der Produktion.

Auch die dritte Prüfungsstufe, die sich auf die Interessensabwägung bezieht, bedarf der getrennten Untersuchung nach Normalbetrieb und Evakuierungsfall.

Im Normalbetrieb besteht, wie oben erläutert, kein berechtigtes Interesse der M AG an der Ortung der Personen im Betrieb. Dem gegenüber steht eine annähernde Totalüberwachung der Beschäftigten, wenn auch mit der Einschränkung, dass es sich nur um Orts- und Bewegungsdaten handelt, nicht aber um Videoaufzeichnungen mit Daten, die auch visuelle Informationen enthielten. Dennoch wird auch eine solche Ortung im Regelfall, wenn also keine Räumung des Gebäudes nötig ist, als unzulässig angesehen.[71]

Im Notfall jedoch könnte die Abwägung anders ausfallen. Das Interesse der Firma an einer schnellen Evakuierung mit den oben ausgeführten positiven Folgen für die M AG ist hier hoch zu gewichten, da der Vorgang der Ortung und die damit verbundenen Suchzeitverkürzungen wesentliche Auswirkungen haben können. Würden Suchzeiten unnötig verlängert, kann dies verschiedene Folgen auslösen, die letztendlich Auswirkungen auf den Fortbestand der Firma haben können.

Gleichzeitig wird der Eingriff in die Persönlichkeitsrechte der Beschäftigten reduziert. Im normalen Geschäftsbetrieb ist das ständige Orten ihrer Aufenthaltsorte und -Wege mit einem latenten Überwachungsdruck verbunden.[72] Im Falle einer notwendigen Evakuierung tritt dieser Gedanke dagegen sowohl objektiv als auch subjektiv zurück.

Die Interessensabwägung müsste also im Evakuierungsfall zugunsten der M AG ausfallen.

Die Betrachtungen zu Art. 6 Abs. 1 f) DSGVO als geeigneter Rechtsgrundlage ergeben also, dass der Betrieb des Ortungssystems nur im Evakuierungsfall hierauf gestützt werden kann. Im normalen Geschäftsbetrieb fehlt es einerseits an einem berechtigten Interesse der M AG, zusätzlich kann nur im Notfall eine Interessensabwägung zugunsten des Arbeitgebers ausfallen.

---

[71] *Maschmann*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, § 26 BDSG Rn. 52.
[72] Analog zum Überwachungsdruck bei Videoüberwachung: *Dendorfer-Ditges*, in: *Moll*/*Altenburg*/*Bengelsdorf*, Münchener Anwaltshandbuch Arbeitsrecht, Teil G. § 35 Rn. 186.

Es findet sich also zum Dauerbetrieb des Ortungssystems im Produktionsbereich keine datenschutzrechtliche Grundlage, während im Evakuierungsfall sowohl Art. 6 Abs. 1 b) als auch f) DSGVO den Einsatz rechtfertigen würden.

b) Ortung von Beschäftigten - Mitbestimmungsrecht des Betriebsrates gem. § 87 Abs. 1 Nr. 6 BetrVG

Gem. § 87 Abs. 1 Nr. 6 BetrVG könnte der Betriebsrat auch im Fall Einführung der Ortung ein Mitbestimmungsrecht haben.

Dazu müsste das System als technische Einrichtung dazu geeignet[73] sein, das Verhalten oder die Leistung der Beschäftigten zu überwachen.

Fraglich ist, ob der Aufenthaltsort und ggf. zurückgelegte Wegstrecken innerhalb des Gebäudes in die Definition von „Verhalten" passen. Wenn, wie in Teil 2 C II 1. b) ausgeführt, jegliches „Tun oder Unterlassen" im Arbeitsumfeld als „Verhalten" zu definieren ist, so ist der Aufenthalt an Orten bzw. das Zurücklegen von Wegstrecken dorthin in die Definition von „Verhalten" einzuordnen.

Auch der Begriff der „Überwachung" i.S.d. Norm dürfte hier greifen, da er, wie in Teil 2 C. II. 1. b) dargelegt, restriktiv auszulegen ist und bei einer durch technische Vorrichtungen automatisch ausgeführten Feststellung von personenbezogenen Zuständen und Gegebenheiten in jedem Fall anwendbar ist.

Dementsprechend ist festzustellen, dass bei der Einführung von Ortungssystemen in der Literatur generell ein Mitspracherecht gesehen wird.[74]

Aufgrund der Eignung des Systems zur Überwachung des Verhaltens der Beschäftigten ist der Betriebsrat der M AG bei der Einführung des Ortungssystems gem. § 87 Abs. 1 Nr. 6 BetrVG mitspracheberechtigt.

III. Zwischenfazit

1. Fall „Gebäudedigitalisierung zum Energiemanagement"

Im Fall des Smart Buildings ergab die Untersuchung der einzelnen funktionalen Bestandteile des Systems, dass Kernfunktionen wie Stammdatenspeicherung, das Speichern der bevorzugten Temperatur- und Lichteinstellungen sowie die

[73] Die Eignung zur Kontrolle von Leistung oder Verhalten reicht bereits aus, eine Bestimmung dazu ist nicht notwendig, s. Teil 2 B III 2 a) bb) „Smart Building – Mitbestimmungsrecht des Betriebsrates gem. § 87 Abs. 1 Nr. 6 BetrVG"

[74] *Däubler*, Gläserne Belegschaften, §6 Rn. 324; für GPS-Ortung analog: *Richardi/Maschmann*, in: *Richardi*, Betriebsverfassungsgesetz mit Wahlordnung, §87 BetrVG Rn. 188.

anwesenheitsabhängige Steuerung von Beleuchtung und Temperatur gesetzlich zulässig sind. Besonders fortschrittliche Funktionen wie die Personen-Zustandserkennung jedoch sind nicht mit den Vorschriften der DSGVO vereinbar.

Eine weitere Hürde für die Einführung des Systems ist, dass der Betriebsrat in der angedachten Ausführung auch der gesetzlich zulässigen Funktionen dem System ablehnend gegenübersteht, da die Einführung einer technischen Basis für erweiterte Kontrollmaßnahmen befürchtet wird.

Die E GmbH sieht sich damit dem Zielkonflikt ausgesetzt, einerseits gesetzlichen Vorschriften der Energieersparnis Genüge zu tun, gleichzeitig Kosten zu senken und so den Bestand der Firma zu sichern und auf der anderen Seite ein konsensfähiges System zu präsentieren, das das Vertrauen der Belegschaft und ihrer Vertretungsorgane genießt.

2. Fall „Personenortung in Gefahrenbereichen“

Beim geplanten Ortungssystem in den beiden Unternehmensbereichen „Kranlager“ und „Produktion“ wäre generell eine Reduktion der Speicherdauer (Kranlager) bzw. eine fallselektive Aktivierung (Produktion) erforderlich, um einen gesetzeskonformen Betrieb zu ermöglichen.

Zusätzlich ist auch hier der Betriebsrat der Einführung gegenüber abgeneigt, wobei seine Bedenken durch negative Erfahrungen mit dem Personalleiter in Sachen Kontrollintensität befeuert werden.

Ähnlich wie im Fall „Smart Building“ steht die M AG auch hier in einem Spannungsfeld; dieses bildet sich aus akut verstärkten rechtlichen Anforderungen, die Arbeitssicherheit zu erhöhen, dabei datenschutzrechtliche Anforderungen zu beachten und schließlich die Zustimmung des Betriebsrates für das technische Gesamtkonzept einzuholen.

3. Abstraktion: Gemeinsamkeiten beider Use Cases

Beide Firmen stehen vor der schwierigen Aufgabe, dass datenschutz- und kollektivarbeitsrechtliche Hindernisse der Einführung eines Systems entgegenstehen, das ansonsten wesentliche Vorteile für alle Beteiligten hätte. Im Fall „Smart Building“ wäre dies ein Komfortgewinn für die Beschäftigten und eine maximale energetische Einsparung für die Firma, im Fall „Ortung“ wäre es die Erhöhung der Arbeitssicherheit mit allen Nebenaspekten auch wirtschaftlicher Art.

Alle genannten Vorteile haben allerdings auch ihren Preis; er würde in beiden Fällen in Form der Verarbeitung von Personendaten erhoben. Die Betroffenen, hier die Beschäftigten bzw. ihre Vertretung, sehen vor allem abstrakte Vorteile, aber einen gefühlt erhöhten Kontrolldruck, was der Grund für eine kritische Haltung ist.

4. Dilemma „Funktion vs. Datenschutz“

Aus den Gemeinsamkeiten beider Fälle tritt ein weiteres Problem hervor, das in einer verstärkt digitalisierten Arbeitswelt aus datenschutzrechtlicher Sicht zunehmend Probleme bereiten kann. Es ist die Kompatibilität von Hard- und Softwareprodukten zu Datenschutz-Vorschriften. In beiden Usecases tritt das Problem in der Form zu Tage, dass nach der Eingrenzung der Produkte, die die erforderlichen Funktionen bieten, kein Produkt mehr in der Auswahl ist, das in seiner vom Hersteller vorgesehenen Betriebsart datenschutzkonform arbeitet.

Beide Firmen sind somit einem Zielkonflikt ausgesetzt. Sie müssen ihren Unternehmenszielen und rechtlichen Verpflichtungen nachkommen können und andererseits eine weitere Rechtspflicht, nämlich die Einhaltung datenschutzrechtlicher Normen, nicht einhalten. Fraglich ist also generell, was zu geschehen hat, wenn sich während der Marktrecherche herausstellt, dass alle ansonsten funktional geeigneten Produkte nicht datenschutzkonform arbeiten, so wie es in beiden geschilderten Usecases der Fall ist.

Zwar könnte ein betroffenes Unternehmen entgegnen, die ausgewählten Produkte gäben nicht mehr Datenschutz her und dies liege außerhalb ihres Einflussbereiches, doch darauf kommt es nicht an. Der Maßstab des umzusetzenden Niveaus an Datenschutz richtet sich nämlich gem. Art. 25 Abs. 1 DSGVO nach dem im Rahmen der Verhältnismäßigkeit Möglichen, also dem „Stand der Technik“, nicht nach dem gerade verfügbaren Stand der ausgewählten Werkzeuge.[75] Beide Firmen können sich, da sie Normadressat sind, auch nicht auf eine Verantwortlichkeit des Software- bzw. Systemherstellers berufen.[76] Dieses wäre nur unter zusätzlichen, hier nicht vorliegenden Bedingungen denkbar.[77]

[75] *Martini*, in: *Paal*/*Pauly*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, DSGVO Art. 25 Rn. 36.
[76] *Hartung*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, DSGVO Art. 25 Rn. 12.
[77] *Hartung*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, DSGVO Art. 25 Rn. 13.

Dieses Dilemma hat auch die Politik erkannt. In einem Entschlussantrag aus Februar 2024[78] regt der Bundesrat unter Punkt 12 eine Verpflichtung der Hersteller an, ausschließlich datenschutzkonforme Produkte auf den Markt zu bringen. Aus technischer Sicht scheint dies ein schwer lösbares Unterfangen zu sein, denn praktisch jedes Produkt kann trotz einer möglichen Datenschutz-Zertifizierung so verwendet werden, dass es nicht mehr datenschutzkonform arbeitet, z.B. indem in Freifeldern Informationen gespeichert werden, deren Inhalt oder Aufbewahrungsfrist den Vorschriften der DSGVO oder des BDSG zuwiderlaufen. Eine Lösung könnten zukünftig KI-Funktionen sein, die selbstständig die datenschutzkonforme Nutzung von Systemen überwachen, da sie in der Lage sind, nach entsprechendem Training kritische Muster zu erkennen.

In der vorliegenden Fallkonstellation jedoch stehen den Unternehmen aus den Usecases solche Produkte bzw. Instrumente nicht zur Verfügung. Fraglich ist also, wie der bestehende Zielkonflikt in beiden Fällen gelöst werden kann.

IV. Maßnahmen zur Lösung der identifizierten Problembereiche

In beiden geschilderten Usecases besteht die Problematik darin, dass personenbezogene Daten anfallen, obwohl sie für den Anwendungsfall weitestgehend nicht erforderlich wären.[79] Dies ist gleichzeitig ein vielversprechender Ansatzpunkt zur Lösung: Wenn es gelänge, die Daten mit Personenbezug zu anonymisieren oder eine Entstehung von Daten mit Personenbezug zu vermeiden, wären die Hindernisse für einen rechtskonformen Betrieb der geplanten Systeme beseitigt, da anonymisierte bzw. anonyme Daten[80] keinen Personenbezug aufweisen und nicht in den Anwendungsbereich der DSGVO fallen.[81]

Könnte man die Systeme zudem so ausgestalten, dass personenbezogene Daten gar nicht entstehen, so dass sie nicht erst anonymisiert werden müssen, würde dies die

[78] N.N., Entschließung des Bundesrates zum 2024 vorgesehenen Bericht der Europäischen Kommission über die Bewertung und Überprüfung gemäß Artikel 97 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (https://www.bundesrat.de/SharedDocs/drucksachen/2023/0601-0700/639-23(B).pdf, abgerufen am 13.03.2024).

[79] Eine Ausnahme ist die Ermittlung der georteten Person im Kranlager im Fall „Ortung“ zu Zwecken der etwaigen Sicherheitsschulung; auf diese Ausnahme wird weiter unten eingegangen.

[80] Im Folgenden soll unterschieden werden zwischen **anonymen** Daten, die von ihrer Entstehung an keinen Personenbezug aufweisen, und **anonymisierten** Daten, die zuvor aus personenbezogenen Daten anonymisiert werden mussten.

[81] Zu anonymisierten Daten: *Scholz*, in: *Simitis*/*Hornung*/*Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG, Art. 4 Nr. 1 DSGVO Rn. 19 f. Analog gilt dies für anonyme Daten, da zu keiner Zeit Personenbezug vorlag.

datenschutzrechtliche Betrachtung weiter vereinfachen. Die häufig vertretene, aber umstrittene Meinung, eine Anonymisierung von Daten stelle einen Vorgang dar, der wiederum auf Art. 6 DSGVO gestützt werden müsse[82], würde in dem Fall von vornherein nicht greifen.

Gleichzeitig erübrigte sich mangels Eignung der Systeme zur Verhaltens- oder Leistungskontrolle das Mitbestimmungsrecht des Betriebsrates.

1. Lösungsansätze „Smart Building“

Ein Workshop mit dem beauftragten Gutachter, der Entwicklungsabteilung des Herstellers und dem Datenschutzbeauftragten der E GmbH ergibt, dass durch einige Änderungen am Konzept eine anonyme Nutzung der Effizienz- und Komfortfunktionen möglich ist.

In dem neuen Konzept werden keine Benutzer-Accounts auf dem Server mehr benötigt. Stattdessen werden die bevorzugten Einstellungen für Helligkeit und Temperatur in der App, die sich jeder Beschäftigte auf sein Diensthandy laden kann, gespeichert. Die App funktioniert ohne Anlage eines Benutzer-Accounts. Sie legt alle Daten verschlüsselt im Handy ab und ist mit einer zusätzlichen PIN gegen unbefugten Zugriff z.B. durch Support-Mitarbeiter geschützt. Per Bluetooth, also auf direktem Wege und ohne Nutzung des Servers, kann ein Nutzer an seine Arbeitsplatzleuchte und sein Raumthermostat die gewünschten Zielwerte übermitteln, indem er Helligkeit und Temperatur auf einem Schieberegler einstellt. Dazu muss er zuvor per QR-Code, die auf den Geräten angebracht sind, seine App mit den Geräten koppeln. Dieser Vorgang ist vom Server unabhängig und findet nur zwischen Handy und Zielgerät statt.

Die Arbeitsplatzleuchte wird demnach zukünftig direkt vom Handy des Nutzers gesteuert. Der Server ist an dieser Kommunikation nicht beteiligt.

Das Raumthermostat erhält zukünftig ebenfalls direkt die Steuerbefehle vom Handy des Nutzers. Kommen von mehreren Handys ggf. unterschiedliche Temperaturbefehle, bildet das Thermostat aus allen den Mittelwert, so wie es ursprünglich der Server auch gesteuert hätte. Die Funktionalität wird also nicht beeinträchtigt.

Der Vorteil der Bluetooth-Verbindung ist in diesem Fall, dass sie nur eine geringe Reichweite hat. Alle gesteuerten Geräte bemerken das Verlassen des Raumes damit

[82] *Roßnagel*, ZD 2021, 188 (189); dagegen: *Thüsing*, ZD 2021, 548 ff.

durch den Abbruch der Verbindung bzw. die Anwesenheit einer bestimmten Person durch eine bestehende oder wiederhergestellte Verbindung. Aus diesem Grund kann auch der Anwesenheitssensor an jedem Schreibtisch entfallen.

Fraglich ist, wie die Speicherung der Komfortwerte in der App datenschutzrechtlich zu bewerten ist. Die Daten wären gem. EG 26 S. 5 DSGVO anonym, wenn sie keinen Bezug mehr zu einer identifizierbaren Person aufwiesen. Dies ist im überarbeiteten Konzept gegeben. Durch eine accountfreie Nutzung und jegliche Entkopplung der Daten in der App von sonstigen personenbezogenen Daten auf dem Handy, z.B. der Apple- oder Android-ID, ist in der Praxis keine Identifizierbarkeit des Nutzers möglich.

Allerdings könnte noch der kombinierte Anwesenheits- und Helligkeitssensor, der die Raumbeleuchtung steuert, bei einer Meldung an den Server theoretische Rückschlüsse auf eine Anwesenheit einzelner Personen zulassen. Auch dieser Sensor sendet daher zukünftig direkt seine Befehle an die Raumbeleuchtung, ohne dass diese Information den Server erreicht. Somit ist auch diese Funktion ohne möglichen Personenbezug umsetzbar.

Es entsteht zusätzlich die Frage zum finanziellen Aufwand für die notwendigen Änderungen am Konzept; die E GmbH könnte sich ggf. auf unangemessen hohe Kosten berufen, deren Verhältnis zum Nutzen nicht gewahrt ist.[83] Da der Hersteller jedoch interessiert am Abschluss des Geschäftes ist, sagt er die Umsetzung der angefragten Funktion ohne Aufpreis zu. Es entstehen daher zur anonymen Nutzung des Systems lediglich interne Prozesskosten, deren Höhe gering ist.

Mit der Anpassung einher geht auch eine Weiterentwicklung des „Standes der Technik“ in der Form, dass nunmehr die Erfordernis der Speicherung der Benutzerstammdaten entfällt. Eine erneute Begutachtung der möglichen Rechtsgrundlage Art. 6 Abs. 1 f) DSGVO für eine Speicherung der Benutzerstammdaten würde also in Kenntnis der neuen Version der Software zu dem Ergebnis kommen, dass die Erforderlichkeit zur Speicherung der Benutzerstammdaten wegfällt und sie nicht auf diese Norm gestützt werden könnte.

[83] *Conrad*, in: *Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, S. 1697 Rn. 226; das Mitspracherecht des Betriebsrates wird allerdings vom Ergebnis der Abwägung nicht berührt und wäre auch dann eine Hürde für die Einführung des Systems, wenn die rein datenschutzrechtliche Abwägung von Kosten und Nutzen zugunsten der E GmbH ausfiele.

Ein weiteres Hindernis zur anonymen Nutzung ist im ursprünglichen Planungsstand noch die Übertragung der persönlichen Terminkalender in den Smart-Building-Server zur termingerechten Klimatisierung von gemeinschaftlich genutzten Räumen, z.B. Konferenzräumen. Diese Steuerung anhand der Ressourcenkalender wird in der Form modifiziert, dass der Smart-Building-Server nur noch eine Information enthält, dass eine Belegung zu einem bestimmten Zeitpunkt geplant ist. Die Information, wer sie gebucht hat und an dem Termin teilnimmt, wird aus der Datenübertragung entfernt. Es liegen dem Smart-Building-Server daher zu keiner Zeit personenbezogene Daten im Zusammenhang mit solchen Buchungen vor.

Der Server dient im überarbeiteten Konzept nur noch der zentralen Gebäudesteuerung. Sämtliche Einstellungen sind zentral zu setzen, jedoch aus Datenschutzgründen nicht zu lesen. Lediglich eine Quittierung eines serverseitig neu gesetzten Wertes wird aus Gründen der Transaktionssicherheit übertragen. So ist trotz der Möglichkeit der zentralen Gebäudesteuerung und voll beibehaltener Komfortfunktionen ein anonymer Betrieb des Systems möglich.

Zum anonymen Betrieb der kamerabasierten Personen-Zustandserkennung in gemeinschaftlich genutzten Räumen bietet der Hersteller ein Ergänzungsmodul der KI-Software an. Dieses ermöglicht eine anonyme Analyse des Zustandes der im Raum befindlichen Personen. Alle von der Kamera erfassten Menschen werden bereits vom Bildverarbeitungsprozessor der Kamera unkenntlich gemacht („Blurring“). Hierdurch wird kein Originalbild von Personen mehr gespeichert. Es findet lediglich im Arbeitsspeicher des Bildverarbeitungsprozessors ein Verarbeitungsprozess statt. Bei dem Prozess wird nicht nur das Gesicht, sondern auch der gesamte Körper komplett verpixelt. Um einen Rückschluss auf die Personen anhand der Statur oder der Kleidung auszuschließen, wird stets ein einheitlich hoher und breiter Bereich um die Person herum derart unkenntlich gemacht und das Bild wird von Farbinformationen befreit. Die Umgebung, also der Hintergrund des Raumes, wird ebenfalls verpixelt. Diese Maßnahmen dienen dazu, auch einen indirekten Personenbezug auszuschließen und vollständige Anonymität i.S.d. DSGVO herzustellen.[84] Körper und Gliedmaßen werden durch einheitliche Striche ersetzt, damit die Aufnahmen bei unklarem Erkennungsergebnis der Personenzustände ohne Einschränkungen zur etwaigen manuellen Auswertung weitergegeben werden können.

[84] Zur Anonymisierung durch Blurring von Videosequenzen: *Hense*, in: *Taeger/Pohle*, Computerrechts-Handbuch, 33.2 Rn. 53.

Hier wäre allerdings der Einwand möglich, dass die Bilder für diesen Prozess im Arbeitsspeicher der Kamera abgelegt werden. Dies könnte einen der DSGVO unterworfenen, rechtfertigungsbedürftigen Vorgang der Datenverarbeitung darstellen.[85] Selbst wenn man dieser umstrittenen Argumentation aber grundsätzlich folgen würde, wäre sie bei diesem Verarbeitungsprozess nicht sinnvoll anwendbar. Der Begriff der Speicherung im Sinne der Datenschutzvorschriften bezieht sich nämlich nicht auf die flüchtige Zwischenspeicherung im Arbeitsspeicher, sondern auf die Vorrätighaltung von Daten zum späteren Abruf.[86] Dagegen könnte man wiederum einwenden, es komme nicht auf die Speicherung, sondern auf die Bearbeitung des Bildes an, das schließlich durch den Prozessor der Kamera anonymisiert werde. Jedoch ist hierauf zu erwidern, dass anhand der fortschreitenden technischen Möglichkeiten, wie sie hier angewandt werden, der traditionelle Begriff der „Verarbeitung“ einer Präzisierung bedürfte. Das Pixelmuster, das auf dem Sensor der Kamera durch die Linse abgebildet wird, mündet zu keinem Zeitpunkt in ein klassisches Bild mit Personenbezug, sondern wird direkt in ein abstraktes Muster ohne Personenbezug umgewandelt, bevor es, falls nötig, zu Lernzwecken weitergeleitet wird. Ist dies nicht notwendig, wird lediglich der erkannte Zustand der Personen in Textform an den Smart-Building-Server weitergeleitet. Es ist bei dem Vorgang innerhalb der Kamera also nicht von einem rechtfertigungsbedürftigen Vorgang der Verarbeitung von Personendaten auszugehen.

Um das Sicherheitskonzept organisatorisch weiter zu optimieren, wird das Login-Verfahren des Smart-Building-Servers auf insgesamt vier Faktoren erweitert. Damit ist gemeint, dass ein Login in das System immer durch zwei Personen, davon mindestens ein Betriebsratsmitglied oder aber der Datenschutzbeauftragte, geschieht (Faktor 1 und 2). Jeder Benutzer, der sich einloggt, erhält zusätzlich per Authentifizierungs-App auf seinem Handy einen Code, der beim Login zusätzlich zum Passwort einzugeben ist (Faktor 3 und 4). Mit der letztgenannten Maßnahme wird sichergestellt, dass kein Passwort-Missbrauch möglich ist. Durch das Vier-Augen-Prinzip ist gewährleistet, dass Veränderungen am System, die die Sicherheit kompromittieren, nicht durch eine Person allein durchgeführt werden können.

[85] *Roßnagel*, ZD 2021, 188 (189); dagegen: *Thüsing*, ZD 2021, 548 ff.

[86] Zur Auslegung v. Art. 4 Nr. 2 DSGVO: *Leopold*, in: *Körner* et al., BeckOGK zum SGB, SGB X § 67 Rn. 29 - die Ablage im Arbeitsspeicher einer EDV-Anlage erfüllt mangels Dauerhaftigkeit nicht die Definition des Speicherns.

Durch die nunmehr anonyme Nutzung ist der Betrieb des Smart Building Servers datenschutzrechtlich nicht mehr limitiert. Auch ein Mitspracherecht des Betriebsrates entfällt, da keine Leistungs- oder Verhaltenskontrolle mit dem System mehr möglich ist.

2. Lösungsansätze „Ortung von Beschäftigten“

Bezüglich der anonymen Nutzung der bisher angedachten personenbezogenen Ortung im Kranlager und im Produktionsbereich ist zunächst zu unterscheiden, welche Teilfunktionalitäten in anonymer Form ebenso ihren Zweck erfüllen würden und welche Funktionen nur in personenbezogener Form sinnvoll sind.

Zur Feststellung, dass sich eine Person im Gefahrenbereich des Kranes aufhält, ist nicht von Belang, um wen es sich handelt. Praktisch alle angedachten Features des Systems wie das Umfahren des Aufenthaltsortes sind auch ohne Kenntnis der individuellen Person umsetzbar. Es gibt hier allerdings eine Ausnahme, nämlich bei der Feststellung, wer möglicherweise entgegen den Sicherheitsvorschriften gehandelt hat und ggf. eine entsprechende Nachschulung erhalten soll. Im Falle einer Anonymisierung der Ortungsfunktionen müsste hier eine alternative Lösung zur Beibehaltung dieser Möglichkeit gefunden werden.

In Bezug auf die Ortung hilfloser Personen im Unglücksfall ist ebenfalls nicht entscheidend, wer geortet wurde. Ein vollständig anonymer Betrieb würde auch diese Funktion nicht beeinträchtigen.

Wenn also eine Lösung für die Funktionalität „Identifizierung zur Sicherheitsnachschulung“ gefunden würde, wäre eine vollständige anonyme Nutzung des Ortungssystems möglich. Hierzu wird mit dem Betriebsrat und der Datenschutzbeauftragten die Möglichkeit besprochen, die Zugangsmöglichkeiten zum Kranlager mit Videokameras zu überwachen. Da es sich um jeweils nur wenige m² überwachter Fläche handelt, in denen zudem in aller Regel niemand arbeitet oder sich aufhält, bestehen seitens des Betriebsrates und des Datenschutzbeauftragten keine Bedenken, sofern die Aufzeichnungszeiten sich im notwendigen Rahmen halten.

Aus datenschutzrechtlicher Sicht könnte in diesen Bereichen ebenfalls eine Videoüberwachung zulässig sein. Hier greift die gleiche Argumentation wie bei der positiven Prüfung der Zulässigkeit der Ortung im Kranlager gem. Art. 6 Abs. 1 f) DSGVO. Die M AG kann sich gem. dieser Norm auf überwiegende, berechtigte Interessen zur Verringerung von Arbeitsunfällen berufen. Dem gegenüber stehen

zwar Eingriffe in das Persönlichkeitsrecht der per Video erfassten Personen, doch ist die Eingriffsintensität durch die örtliche Eingrenzung auf den Zugang zu einem Gefahrenbereich quantitativ stark verringert bei gleichzeitig erhöhtem Gefahrenpotenzial.

Auch aus gesetzlicher Sicht bestehen also bei diesem begrenzten Einsatz von Videokameras keine Bedenken.

Bezüglich der Speicherdauer der Aufnahmen ist zu beachten, dass sie gem. Art. 17 Abs. 1 a) DSGVO auf die notwendige Zeit zu begrenzen ist. Hier ist geplant, dass die Aufzeichnung automatisch beginnt, sobald jemand von den Kameras erfasst wird. Eine Stunde nach dem Ende jeder Schicht werden die Aufnahmen gelöscht, sofern niemand mehr im Kranlager geortet wird und in der entsprechenden Schicht kein Alarm ausgelöst wurde, also keine Identifikation von Personen mehr notwendig ist. Auch dieser Regelung stimmen der Betriebsrat und die Datenschutzbeauftragte zu.

Nachdem nun eine Lösung für die fallweise Identifikation von Personen im Kranlager gefunden wurde, ist fraglich, wie eine anonyme Nutzung der zu ortenden BLE-Tags sichergestellt werden könnte. Dabei ist aus datenschutzrechtlicher Sicht eine Lösung dann als anonym anzusehen, wenn sie technisch und organisatorisch so ausgelegt ist, dass zu keinem Zeitpunkt Daten mit Bezug zu einer bestimmbaren Person entstehen.[87] Dieses Ziel entspricht, sofern es technisch und organisatorisch umsetzbar ist, sowohl dem Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 c) DSGVO[88] als auch der Vorgabe „Privacy by Design“ aus Art. 25 Abs. 1 DSGVO.[89]

Übertragen auf den Fall des Ortungssystems wäre also der Idealfall, dass bereits das am Körper getragene BLE-Tag keine eindeutige ID mehr sendet. Technisch ist dies jedoch nicht möglich, da jedes Bluetooth-Device weltweit eine eindeutige, nicht änderbare ID („MAC-ID“) besitzt, die mit der Fahrgestellnummer eines Fahrzeugs vergleichbar ist und die die Grundlage der Kommunikation des Bluetooth-Standards ist. Diese Option der Anonymisierung scheidet also aus.

[87] Zur Definition anonymer Daten: *Klar/Kühling*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 4 Nr. 1 DSGVO Rn. 31 ff.
[88] Zu den einzelnen Kriterien der Datenminimierung: *Reimer*, in: *Sydow*/*Marsch*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 5 DSGVO Rn. 32.
[89] In Bezug auf "Datenschutz 'by design'" in IT-Infrastrukturen: *Herberger*, in: *Weth* et al., Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, S. 116 Rn. 25.

Dieses Problem ist jedoch organisatorisch lösbar. Statt persönlich zugeordneter BLE-Tags wird eine Aufbewahrungs- und Aufladestation am Personaleingang vorgesehen, aus der die Beschäftigten beim Zutritt zum Produktionsbereich ein zufällig ausgewähltes BLE-Tag entnehmen und nach Schichtende wieder in einen beliebigen Ladeschacht einstecken können. Hierdurch ergibt sich, dass keine feste Zuordnung zwischen BLE-Tag und Person mehr besteht. Ein weiterer Vorteil in der Nutzungspraxis ist, dass die BLE-Tags in der Station stets aufgeladen werden und ihre Funktion sichergestellt wird.

Dennoch wäre es theoretisch denkbar, dass ein fachkundiger Administrator sich Zugang zu personenbezogenen Daten in der Art verschafft, dass er eine bestimmte Person beim Betreten des Gebäudes beobachtet und Informationen über die ID des von der Person mit sich geführten BLE-Tags ausspäht. Am Ende der Arbeitsschicht könnte so ein Bewegungsprofil rekonstruiert werden. Es lägen also personenbezogene Daten im System vor.

Um dies zu vermeiden, wird vom Hersteller auch eine Modifikation an der Firmware[90] der Basisstationen vorgenommen. Diese verändern fortan die IDs der empfangenen BLE-Tags nach einem sicheren Verfahren, so dass ab diesem Punkt der Verarbeitungskette kein Bezug mehr zum BLE-Tag und damit zur georteten Person möglich ist.[91]

Um jegliche Rekonstruktion zurückgelegter Wege auszuschließen, wird auch der Standortverlauf eines jeden BLE-Tags nicht mehr, so wie ursprünglich im Systemstandard vorgesehen, gespeichert. Sobald neue Ortungsdaten vorliegen, werden die vorherigen gelöscht.

Der Hersteller des Systems, der interessiert an der Projektumsetzung und an der datenschutzkonformen Auslegung seiner Produkte ist, bietet in diesem Fall die notwendigen Modifikationen an der Software des Gesamtsystems als zusätzliche Leistung ohne Aufpreis an. Das in Art. 25 Abs. 1 DSGVO festgelegte Gebot der Verhältnismäßigkeit aus Aufwand und Nutzen auf Seiten des Verantwortlichen bleibt also gewahrt.

[90] S. Glossar.

[91] Damit das Ortungsverfahren auch weiterhin funktioniert, müssen die IDs der BLE-Tags von allen Basisstationen auf einheitlichem Wege verschlüsselt werden. Dies geschieht mit einer sog. „Unumkehrbaren Kryptologischen Hashunktion“ im SHA-2-Verfahren. Details s. Glossar

Auch auf der organisatorischen Seite sind Optimierungen zugunsten des Datenschutzes angezeigt. So ist es ungünstig, dass der Personalleiter weisungsbefugt gegenüber denjenigen ist, die Zugriff auf sensible Daten, z.B. die Videoaufzeichnungen der Kameras am Kranlager, besitzen. Es wird daher vereinbart und im Prozesshandbuch des Unternehmens dokumentiert, dass Zugriffe auf Systeme, die personenbezogene Daten enthalten, deren Informationsgehalt über reine Abrechnungszwecke hinausgeht, nach dem Vieraugenprinzip erfolgen sollen. Die Rechtevergabe wird derart ausgestaltet, dass immer ein Mitglied des Betriebsrates oder die Datenschutzbeauftragte einen der zwei notwendigen Benutzer zum Login darstellen. Hierdurch wird erreicht, dass ein Personenkreis, der aufgrund seines besonderen Kündigungsschutzes[92] keine Restriktionen befürchten muss, Kontrolle über sensible Datenzugriffe ausübt.

Zudem wird der Zugriff auf die Tablets, die Rettungskräften die Orte von zu bergenden Personen im Gebäude anzeigen, organisatorisch so geregelt, dass keine missbräuchliche Nutzung stattfinden kann.

Im Ergebnis entfällt für das Ortungssystem durch die anonyme Nutzung die Anwendung von Datenschutzvorschriften ebenso wie das Mitbestimmungsrecht des Betriebsrates. Bzgl. der Ausnahme der Video-Identifikation von Personen, die den Gefahrenbereich des Kranlagers betreten, konnte ein ebenso praktikables wie datenschutzkonformes Konzept erstellt werden, das die Zustimmung der Arbeitnehmervertretung findet.

Teil 3: Fazit

A. Zusammenfassung der Betrachtungen

Beide Usecases zeigen, dass abseits der eigentlich gewünschten Daten und Systemfunktionen personenbezogene Daten auch dort entstehen, wo es nicht für die Funktion des System erforderlich wäre. Durch Modifikationen an Organisation und Technik ließen sich jedoch in beiden Fällen die datenschutzrechtlichen Herausforderungen lösen.

Beide Fälle zeigen damit gemeinsame Eigenschaften, die in der Einleitung und der Zielsetzung in Teil 1 vermutet wurden, dass nämlich die Funktionalität von IIoT-Systemen oftmals nicht oder nur in Teilbereichen auf die Erhebung

[92] Der Datenschutzbeauftragte genießt Kündigungsschutz gem. Art. 38 Abs. 3 S. 2 DSGVO, Betriebsratsmitglieder gem. § 15 Abs. 1 S. 1 KSchG

personenbezogener Daten angewiesen ist, diese aber ungewollt im Prozess der Datenverarbeitung entstehen.

Gerade diese Tatsache macht in beiden Fällen eine anonyme Nutzung der IIoT-Systeme möglich. Beachtung verdient dabei, dass bei den Konzepten zur Anonymität in beiden Usecases keine personenbezogenen Daten entstehen, diese also nicht erst anonymisiert werden müssen. Durch eine durchgängige Umsetzung des Grundsatzes „Privacy by Design“ in Verbindung mit organisatorischen Regelungen kann also die Entstehung personenbezogener Daten verhindert und die datenschutzrechtliche Komplexität reduziert werden.

Bei der datenschutzrechtlichen Betrachtung beider Fälle war es zudem hilfreich, die geplanten Systeme in Bezug auf den Datenschutz und kollektivarbeitsrechtliche Regelungen getrennt nach ihren funktionalen Modulen zu betrachten. Es kann sich, wie im Usecase 2 („Ortung von Personen“), nämlich herausstellen, dass bei Teilfunktionalitäten ein Personenbezug erforderlich ist, hier bei der fallweisen Identifikation von Personen im Kranlager. Im vorliegenden Fall hätte dies zur Folge gehabt, dass das gesamte System den Ballast des Personenbezugs tragen müsste, nur um einen geringen Teil der Gesamtfunktionen zu ermöglichen. Stattdessen wurde die Identifikation der betroffenen Personen mit einem separaten Werkzeug (hier der Videoüberwachung) gelöst, um das Hauptsystem anonym betreiben zu können.

Der Vorteil dieser Ausgliederung ist, dass die entstehenden Datenmengen weit geringer und damit die datenschutzrechtlichen Verfahren leichter durchführbar sind. Gleichzeitig ist die Akzeptanz der Betroffenen höher, da die Überwachung sich auf offenbar notwendige Gefahrenzonen fokussiert und nicht der Eindruck der Totalüberwachung entsteht.

B. Handlungsempfehlungen für die Unternehmenspraxis

Die geschilderten Usecases zeigen mehrere Punkte auf, die bei der Planung und Durchführung eines IIoT-Projektes grundsätzlich beachtet werden sollten.

Zunächst ist eine Einbeziehung datenschutzrechtlicher Aspekte während der Produktauswahl und der technischen und organisatorischen Planung des Vorhabens bedeutsam. Dies gewährleistet, dass rechtzeitig entsprechende Problemfelder offenbar werden, die eine organisatorische oder technische Anpassung des Konzeptes erfordern. Würden diese Probleme erst nach dem Erwerb der Systeme oder gar nach der Inbetriebnahme deutlich, wären kostspielige Anpassungen oder die

Abschaltung des Systems erforderlich. Zudem lassen sich erforderliche Modifikationen an Produkten im Auswahlprozess, deren datenschutzrechtliche Auslegung noch verbessert werden muss, oft in dieser Phase noch besser mit den Herstellern verhandeln, als wenn die Kaufentscheidung schon vertraglich besiegelt ist und der Preis für die nachträglichen Änderungen praktisch durch den Hersteller diktiert werden kann. Diese Problematik würde allerdings abgeschwächt, sollten die o.g. politischen Überlegungen bzgl. der herstellerseitigen Verpflichtung zur Einhaltung gesetzlicher Datenschutz-Standards Einzug in die Gesetzgebung halten.

Der zweite wichtige Punkt ist die Abstimmung eines Vorhabens mit den Beschäftigten und ihren Vertretungen. Selbst wenn nämlich der Betrieb eines Systems auf rechtlicher Basis zulässig ist, so muss in fast allen Fällen einer Datenverarbeitung mit Personenbezug eine Zustimmung des Betriebsrates gem. § 87 Abs. 1 Nr. 6 BetrVG eingeholt werden. Eine offene Kommunikation über den Grund, die Ziele und die Ausgestaltung einer geplanten Maßnahme gegenüber der Belegschaft und ihrer Vertretung kann dabei helfen, Vorbehalte gegenüber technischen Systemen, deren Funktionsweise oft nicht ohne Weiteres zu verstehen ist, abzubauen.

Ein dritter Aspekt, der bei vielen IIoT-Projekten grundsätzlich umsetzbar sein dürfte, ist die vollständig anonyme Nutzung der Funktionen. Immer dann, wenn entstehende Daten mit Personenbezug nicht der eigentliche Zweck, sondern nur ungewollte Nebenprodukte sind, empfiehlt es sich, die anonyme Nutzung direkt im Systemdesign zu verankern („Privacy by Design“). Zwar entstehen anfänglich höhere Begutachtungs-, Planungs- und Umsetzungskosten, jedoch kann sich eine solche Maßnahme langfristig auszahlen, indem Datenschutz-Prozesskosten entfallen und potenzielle weitere Probleme beim Umgang mit personenbezogenen Daten vermieden werden.

Stellt man bei der Planung fest, dass eine Teilfunktionalität einen Personenbezug erfordert, sollte geprüft werden, ob diese Funktionalität in ein separates Werkzeug ausgegliedert werden kann, um das geplante Hauptsystem weiterhin anonym betreiben zu können. Hier ist eine Abwägung der Szenarien bzgl. Kosten, Aufwand, Datenschutz- und Kollektivarbeitsrecht notwendig.

Zu beachten ist bei der Einstufung von Daten als „anonym“, dass angesichts der schnellen Weiterentwicklung technischer Analyse- und

Kombinationsmöglichkeiten, zukünftig vor allem durch KI-gestützte Tools, hohe Anforderungen an eine wirksame Anonymisierung bzw. Anonymität zu stellen sind.[93]

Ist eine anonyme Nutzung nicht umsetzbar, kann eine Pseudonymisierung der Daten eine mögliche Maßnahme sein, den Datenschutz zu optimieren und die Akzeptanz der Belegschaft zu erhöhen. Sie hat jedoch den Nachteil, dass pseudonymisierte Daten nach wie vor als solche mit Personenbezug gelten[94] und daher ein entsprechendes Projekt datenschutzrechtlich größere Hürden überwinden muss.

Sobald also personenbezogene Daten nicht oder nur in ausgliederbaren Randbereichen benötigt werden, kann eine anonyme Ausgestaltung von IIoT-Systemen als optimale Lösung für alle Beteiligten betrachtet werden.

[93] *Ernst*, in: *Paal*/*Pauly*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 4 DSGVO Rn. 48 ff.
[94] *Klar/Kühling*, in: *Kühling*/*Buchner*/*Bäcker*, Datenschutz-Grundverordnung, Art. 4 Nr. 5 DSGVO Rn. 11.

Literaturverzeichnis

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl., München 2019 (zit. als *Bearbeiter,* in: *Auer-Reinsdorff/I. Conrad*, Handbuch IT- und Datenschutzrecht).

Brink, Stefan/Wolff, Heinrich A./v. Ungern-Sternberg, Antje (Hrsg.), BeckOK Datenschutzrecht, 46. Aufl., München 2023 (zit. als *Bearbeiter,* in: *Brink/Wolff/v. Ungern-Sternberg*, BeckOK Datenschutzrecht).

Byers/Winkler/Stelter, Zulässigkeit von biometrischen Kontrollen am Arbeitsplatz, NZA 2023, 457 (458).

Calliess, Christian/Ruffert, Matthias/Blanke, Hermann-Josef et al. (Hrsg.), EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta : Kommentar, 6. Aufl., München 2022 (zit. als *Bearbeiter,* in: *Calliess et al.*, EUV/AEUV).

Däubler, Wolfgang, Gläserne Belegschaften, Das Handbuch zum Beschäftigtendatenschutz, 9. Aufl., Frankfurt am Main 2021.

Domínguez-Bolaño, Tomás/Campos, Omar et al., An overview of IoT architectures, technologies, and existing open-source projects, v. 2022 (https://www.sciencedirect.com/science/article/pii/S254266052200107X, zugegriffen am 17.03.2024).

Dornbusch, Gregor/Fischermeier, Ernst/Löwisch, Manfred et al. (Hrsg.), AR - Kommentar zum gesamten Arbeitsrecht, 10. Aufl., Köln 2021 (zit. als *Bearbeiter,* in: *Dornbusch et al.*, AR - Kommentar zum ges. Arbeitsrecht).

Ehmann, Eugen/Selmayr, Martin (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl., München 2018 (zit. als *Bearbeiter,* in: *Ehmann/Selmayr*, Datenschutz-Grundverordnung).

Gola, Peter/Heckmann, Dirk/Brand, Thimo et al. (Hrsg.), Datenschutz-Grundverordnung VO (EU) 2016/679, Bundesdatenschutzgesetz, Kommentar, 3. Aufl., München 2022 (zit. als *Bearbeiter,* in: *Gola et al.*, Datenschutz-Grundverordnung VO (EU) 2016/679, Bundesdatenschutzgesetz).

Hauschka, Christoph E./Moosmayer, Klaus/Lösler, Thomas (Hrsg.), Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, 3. Aufl., Beck-online Bücher, München 2016 (zit. als *Bearbeiter,* in: Corporate Compliance).

Henssler, Martin/Willemsen, Heinz J./Kalb, Heinz-Jürgen (Hrsg.), Arbeitsrecht, Kommentar, 9. Aufl., Köln 2020 (zit. als *Bearbeiter,* in: *Henssler/Willemsen/Kalb*, Arbeitsrecht).

Kaufmann, Muriel/Wegmann, Simon/Wieg, Florian, Beschäftigtendatenschutz - Spielräume und Herausforderungen mitgliedstaatlicher Regelungen, Überlegungen vor dem Hintergrund der Entscheidung des EuGH vom 30.3.2023 - C-34/21, NZA 2023, 740.

König, Tassilo-Rouven, Beschäftigtendatenschutz in der Beratungspraxis, Baden-Baden 2020.

Körner, Anne/Krasney, Martin/Mutschler, Bernd et al. (Hrsg.), beck-online.GROSSKOMMENTAR zum SGB: SGB I, SGB IV, SGB V, SGB VI, SGB VII, SGB X, SGB XI (Kasseler Kommentar), 126. Aufl., München 2024 (zit. als *Bearbeiter,* in: *Körner et al.*, BeckOGK zum SGB).

Kramer, Stefan (Hrsg.), IT-Arbeitsrecht, Handbuch Digitalisierung, Homeoffice, KI, virtuelle Betriebsratsarbeit, 3. Aufl., München 2023 (zit. als *Bearbeiter,* in: S. *Kramer*, IT-Arbeitsrecht).

Kühling, Jürgen/Buchner, Benedikt/Bäcker, Matthias (Hrsg.), Datenschutz-Grundverordnung, 4. Aufl., München 2024 (zit. als *Bearbeiter,* in: *Kühling/*B. *Buchner/Bäcker*, Datenschutz-Grundverordnung).

Marković, Industrielles IoT - Marktdaten-Analyse (https://de.statista.com/statistik/studie/id/146076/dokument/industrielles-iot-marktdaten-und-analyse/, zugegriffen am 18.11.2023).

Moll, Wilhelm/Altenburg, Stephan/Bengelsdorf, Peter (Hrsg.), Münchener Anwaltshandbuch Arbeitsrecht, 5. Aufl., München 2021 (zit. als *Bearbeiter,* in: *Moll/Altenburg/Bengelsdorf*, Münchener Anwaltshandbuch Arbeitsrecht).

N.N., Entschließung des Bundesrates zum 2024 vorgesehenen Bericht der Europäischen Kommission über die Bewertung und Überprüfung gemäß Artikel 97 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (https://www.bundesrat.de/SharedDocs/drucksachen/2023/0601-0700/639-23(B).pdf, zugegriffen am 13.03.2024).

N.N., IDC - Volumen der jährlich generierten/replizierten digitalen Datenmenge weltweit von 2010 bis 2022 und Prognose bis 2027 (in Zettabyte) (https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/, zugegriffen am 04.11.2023).

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., München 2021 (zit. als *Bearbeiter,* in: *Paal/Pauly*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz).

Ramadan, Muawia/Shuqqo, Hana/Qtaishat, Layalee, et al., Sustainable Competitive Advantage Driven by Big Data Analytics and Innovation, Applied Sciences 2020, 6784.

Richardi, Reinhard (Hrsg.), Betriebsverfassungsgesetz mit Wahlordnung, Band 5, 17. Aufl., München 2022 (zit. als *Bearbeiter,* in: *Richardi*, Betriebsverfassungsgesetz mit Wahlordnung).

Robrahn/Bremert, Interessenskonflikte im Datenschutzrecht, ZD, 2018, S. 291, 292.

Rolfs, Christian (Hrsg.), Beck'scher Online-Kommentar Arbeitsrecht, München 2006 (zit. als *Bearbeiter,* in: *Rolfs*, BeckOK Arbeitsrecht).

Roßnagel, ZD 2021, 188 - Datenlöschung und Anonymisierung Verhältnis der beiden Datenschutzinstrumente nach DS-GVO, ZD 2021, 188 (189).

Säcker, Franz J./Rixecker, Roland/Oetker, Hartmut et al. (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, 9. Aufl., München 2023 (zit. als *Bearbeiter,* in: MüKoBGB).

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019 (zit. als *Bearbeiter,* in: *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht - DSGVO mit BDSG).

Sydow, Gernot/Marsch, Nikolaus (Hrsg.), DS-GVO, BDSG, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., Baden-Baden u.a. 2022 (zit. als *Bearbeiter,* in: *Sydow/Marsch*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz).

Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 38. Aufl., München 1990, Stand: August 2023 (zit. als *Bearbeiter,* in: Taeger/Pohle, Computerrechts-Handbuch).

Thüsing, Gregor (Hrsg.), Beschäftigtendatenschutz und Compliance, Effektive Compliance im Spannungsfeld von reformiertem BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, 3. Aufl., München 2021 (zit. als *Bearbeiter,* in: *Thüsing*, Beschäftigtendatenschutz und Compliance).

Thüsing, Rombey, Anonymisierung an sich ist keine rechtfertigungsbedürftige Datenverarbeitung, Eine Auslegung von Art. 4 Nr. 2 DS-GVO nach den Methoden des EuGH, ZD 2021, 548 ff.

Weber, Klaus (Hrsg.), Rechtswörterbuch, 31. Aufl., München 2023 (zit. als *Bearbeiter,* in: *Weber*, Rechtswörterbuch).

Weichert, Die Verarbeitung von Wearable-Sensordaten bei Beschäftigten, NZA 2017, 565 (567).

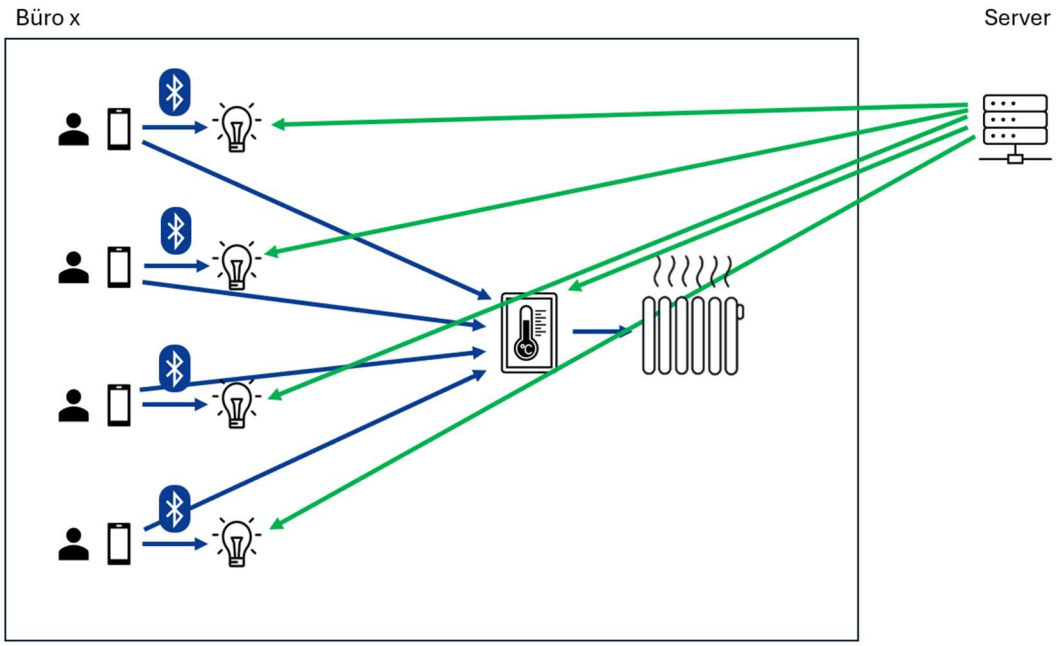
Weth, Stephan/Herberger, Maximilian/Wächter, Michael et al. (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl., Beck-online Bücher, München 2019 (zit. als *Bearbeiter,* in: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis).

Wolff, Heinrich A./Brink, Stefan (Hrsg.), Datenschutzrecht, Grundlagen, Bereichsspezifischer Datenschutz, DS-GVO, BDSG, 2. Aufl., München 2022 (zit. als *Bearbeiter,* in: *Wolff/Brink*, Datenschutzrecht, Bereichsspezifischer Datenschutz, DS-GVO, BDSG).

Anhang 1

Anonyme Umsetzung von Effizienz- und Komfortfunktionen eines Smart-Building-Systems

Ziel ist eine anonyme Nutzung des Smart-Building-Systems bei gleichzeitiger zentraler Steuerbarkeit des Gebäudes. Es gilt, keine nachvollziehbare Verbindung zwischen Nutzer-Transaktionen und einer natürlichen Person zu schaffen. Dazu werden die Aktoren wie Licht-Dimmer und Thermostate auf zwei verschiedenen Wegen angesprochen, so dass Nutzeraktionen keine Datenspuren hinterlassen und Komfort-Einstellungen anonym hinterlegt und genutzt werden können.



Steuerung durch Nutzer:

Anonym gespeicherte Werte werden direkt per Bluetooth an die Zielgeräte übertragen. Es besteht dabei kein Personenbezug.

Steuerung durch Server:

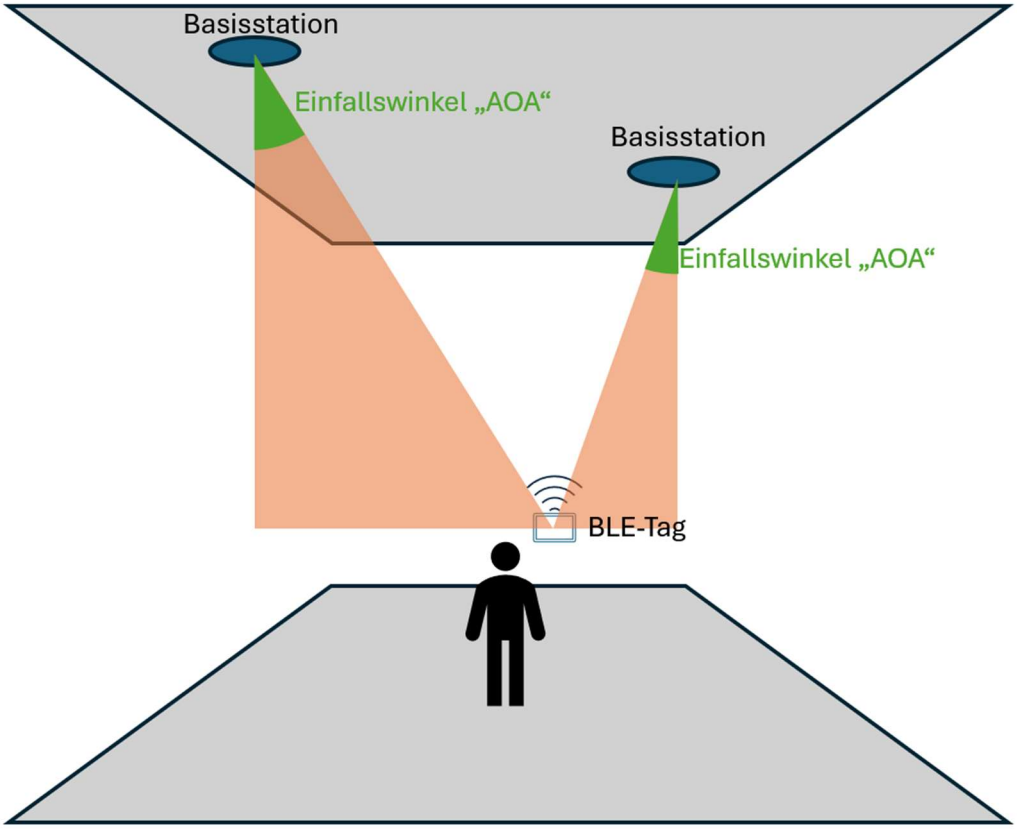
Der Server kann Werte an alle Dimmer und Thermostate setzen, jedoch nicht lesen; hierdurch wird vermieden, dass Rückschlüsse auf Anwesenheiten einzelner Personen oder aktive Komfortwerte in bestimmten Büros ausgelesen werden können.

Anhang 2

Funktionsprinzip der Ortung von BLE-Tags nach dem AOA-Verfahren

Durch die unterschiedlichen Einfallswinkel der Funksignale eines BLE-Tags in die einzelnen Basisstationen ist nach geometrischen Berechnungsverfahren eine Ortung des Senders möglich. Aus Gründen der Übersicht werden hier nur zwei Basisstationen dargestellt; in der Praxis erreicht man ab einer Anzahl von drei Basisstationen, die Signale eines BLE-Tags empfangen können, genaue Ortungsdaten.

Spiel



Eidesstattliche Versicherung

Hiermit versichere ich, Michael Pelster, dass ich die Masterarbeit selbstständig verfasst und weder diese Arbeit noch Teile davon an anderer Stelle zu Prüfungszwecken eingereicht habe, sowie keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Greven, 20.03.2024 Michael Pelster

Ort, Datum Unterschrift