Volker Johannhörster, Matthias Kohn, Thomas Kunz, Janine Schleper, Ulrich Waldmann*

Live-Ortung von Beschäftigten in der agilen Personaleinsatzplanung

Umsetzung des Datenschutzes in der Intralogistik

Unternehmen verarbeiten in der Regel viele personenbezogene Daten ihrer Beschäftigten. Insbesondere werden häufig auch Live-Ortungsdaten der Beschäftigten erhoben. In diesem Beitrag betrachten wir konkrete Anwendungsszenarien in großen Logistikhallen, in denen die Live-Ortungsdaten der Beschäftigten ermittelt werden, um deren Einsatzort dynamisch umplanen zu können. Wir zeigen, wie eine auf Bluetooth Low Energy basierende Live-Ortung datenschutzkonform in die Einsatzplanung integriert werden kann.

1 Problemstellung

Unternehmen verarbeiten in der Regel große Mengen an personenbezogenen Daten über ihre Beschäftigten. Insbesondere im Rahmen der agilen Ressourcenplanung erheben Unternehmen sehr heikle Daten, wie z. B. Geburtsdatum, Verträge, Qualifikationen, Einsätze, Abwesenheiten, Leistungsgrade, etc. ihrer Beschäftigten. Die agile Ressourcenplanung ist jedoch insbesondere in der Logistik von hoher Relevanz, da selbst Ausfallzeiten von 15 bis 30 Minuten eine erhebliche Herausforderung für eine optimale Ressourcenplanung der anwesenden Beschäftigten erfordern. Die Erfassung von Standortdaten der Beschäftigten spielt hierbei eine entscheidende Rolle: Aufgrund der Größe der Firmengelände von bis zu 100.000 Quadratmetern, ist es für Unternehmen häufig unabdingbar genau zu wissen, wann sich ihre Beschäftigten an welchem Standort aufhalten, etwa um denjenigen

* Das diesem Beitrag zugrunde liegende Vorhaben EduMiDa wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 16KIS1361K, 16KIS1362 und 16KIS1542 gefördert. Die Verantwortung für den Inhalt liegt bei den Autor*innen.

Volker Johannhörster

ist Co-Founder und geschäftsführender Gesellschafter der p.l.i. solutions GmbH.

E-Mail: vjohannhoerster@pli-solutions.de

Matthias Kohn

ist wissenschaftlicher Mitarbeiter und Doktorand am Institut für Informations- Gesundheits- und Medizinrecht der Universität Bremen und Rechtsreferendar am Oberlandesgericht Düsseldorf.
E-Mail: kohn@uni-bremen.de

Thomas Kunz

ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie SIT.

E-Mail: thomas.kunz@sit.fraunhofer.de

Janine Schleper

ist wissenschaftliche Mitarbeiterin und Doktorandin am Institut für Informations- Gesundheits- und Medizinrecht der Universität Bremen und Rechtsreferendarin am Hanseatischen Oberlandesgericht in Bremen.
E-Mail: schleper@uni-bremen.de

Ulrich Waldmann

ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie SIT.

E-Mail: ulrich.waldmann@sit.fraunhofer.de

Beschäftigten zur Reparatur einer defekten Anlage bzw. Maschine schicken zu können, der sich örtlich am nächsten an dieser befindet. Häufig ist dem Arbeitgeber auch daran gelegen, zu wissen, mit welcher Tätigkeit ein Beschäftigter gerade beschäftigt ist und wann er mit der aktuellen Tätigkeit begonnen hat, z. B., um abzuschätzen, wie lange die aktuelle Tätigkeit noch andauern wird und wann der Beschäftigte einen neuen Auftrag annehmen kann. Eine agile Ressourcenplanung, die auf Echtzeiterhebungen von Standortdaten beruht, ist somit von hohem wirtschaftlichem Interesse für Unternehmen.

Allerdings können diese Daten zu umfangreichen Persönlichkeitsprofilen aggregiert werden, erst recht, wenn die Beschäftigten zur Erhebung der Standortdaten mit Smart Devices ausgestattet werden, die in der Lage sind, weitere potenziell problematische Daten, wie z. B. den aktuellen Pulswert, zu erheben. Dementsprechend stellt die DSGVO hier hohe Anforderungen an die Rechtmäßigkeit der Datenverarbeitung durch das Unternehmen, um einen Missbrauch der Mitarbeiterdaten vorzubeugen. Wie diese Anforderungen in der Praxis umgesetzt werden können, soll dieser Beitrag zeigen.

2 Anwendungsszenarien aus der Logistik

Im Folgenden werden wir exemplarisch zwei Szenarien vorstellen, bei denen die Erhebung der Standortdaten von Beschäftigten für die Umplanung erforderlich ist: (1) Die Umplanung von Beschäftigten aufgrund eines Technikausfalls und (2) die Umplanung von Beschäftigten aufgrund kurzfristiger Mehrbelastung.

Im ersten Szenario gehen wir davon aus, dass auf einem großen Firmengelände in einer weit entfernten Logistikhalle ein technisches System ausfallen könnte, das für den Logistikbetrieb unerlässlich ist. Im Rahmen einer agilen Personaleinsatzplanung müssen nun folgende Aspekte berücksichtigt werden: Die Anlage muss so schnell wie möglich repariert werden. In jeder Schicht gibt es mehrere Beschäftigte, die in der Lage wären, die Anlage zu reparieren. Durch die Verknüpfung eines Systems zur Personaleinsatzplanung (PEP) mit den Standortdaten der Beschäftigten soll entschieden werden, welcher qualifizierte Beschäftigte der Anlage am nächsten ist und sie somit am schnellsten erreichen und reparieren kann. Reparaturarbeiten können von wenigen Minuten bis zu mehreren Stunden dauern, und die Zahl der Beschäftigten, die diese Aufgabe übernehmen können, ist gering. Hinzu kommt, dass die Beschäftigten, die an der ausgefallenen Anlage gearbeitet haben, kurzfristig andere Aufgaben übernehmen sollen. Insbesondere dann, wenn die Wartezeit wegen der Behebung der technischen Störung voraussichtlich länger als 30 Minuten beträgt, sollen die Beschäftigten an anderen Arbeitsplätzen bzw. Planungseinheiten eingesetzt werden.

Im zweiten Szenario besteht kurzfristig beispielsweise für ca. 15 bis 60 Minuten ein erhöhter Bedarf an Beschäftigten an einem bestimmten Arbeitsplatz. Die dort zu erledigenden Aufgaben können von vorhandenen Beschäftigten, die über die notwendigen Qualifikationen verfügen, übernommen werden. Durch die Berücksichtigung der aktuellen Standorte der Beschäftigten in der PEP soll entschieden werden, welche Beschäftigten dem Ort des Mehrbedarfs am nächsten sind, kurzfristig von ihrem aktuellen Arbeitsplatz abgezogen werden können und somit am schnellsten Unterstützung leisten können.

Darüber hinaus ermöglichen es Systeme zur Standortermittlung von Beschäftigten auf dem Firmengelände, z. B. im Falle einer Gebäudeevakuierung in einem Notfall festzustellen, ob sich noch Personen in dem betroffenen Bereich aufhalten (wichtiges Zusatzszenario).

3 Rechtliche Betrachtung der Szenarien

Bei den Standortdaten von Beschäftigten, sowie deren Qualifikationen, Namen, Personalnummern usw. handelt es sich um personenbezogene Daten, weshalb die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DSGVO erfüllt sein müssen.

Die *Rechtmäßigkeit der Verarbeitung* (Art. 6 Abs. 1 DSGVO) lässt sich in den von uns betrachteten Szenarien mit dem berechtigten Interesse (Art. 6 Abs. 1 lit. f DSGVO) begründen, welches sich aus der Optimierung der Personaleinsatzplanung ergibt (vgl. auch [4]). Voraussetzung hierfür ist allerdings, dass nicht die schutzwürdigen Interessen der Beschäftigten überwiegen. Dies wäre z. B. dann der Fall, wenn aus der Standortbestimmung der Beschäftigten eine permanente Überwachung folgen würde. In unseren Szenarien beschränkt sich die Standortbestimmung auf das Firmengelände und somit nur auf die Arbeitszeit. Zudem sollten die Beschäftigten die Möglichkeit haben, die Standortermittlung beispielsweise während der Pausenzeiten zu deaktivieren. Darüber hinaus kann die Standortbestimmung auch im berechtigten Interesse der Beschäftigten sein, wenn sich damit z. B. feststellen lässt, ob sich in Notfallsituationen Personen in dem betroffenen Bereich des Firmengeländes aufhalten.

Gemäß der *Zweckbindung* (Art. 5 Abs. 1 lit. b DSGVO) müssen die personenbezogenen Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. In den von uns betrachteten Szenarien ergibt sich die Zweckbindung aus der Notwendigkeit der Personalumplanung aufgrund besonderer Ereignisse bzw. aus der Optimierung der Personaleinsatzplanung.

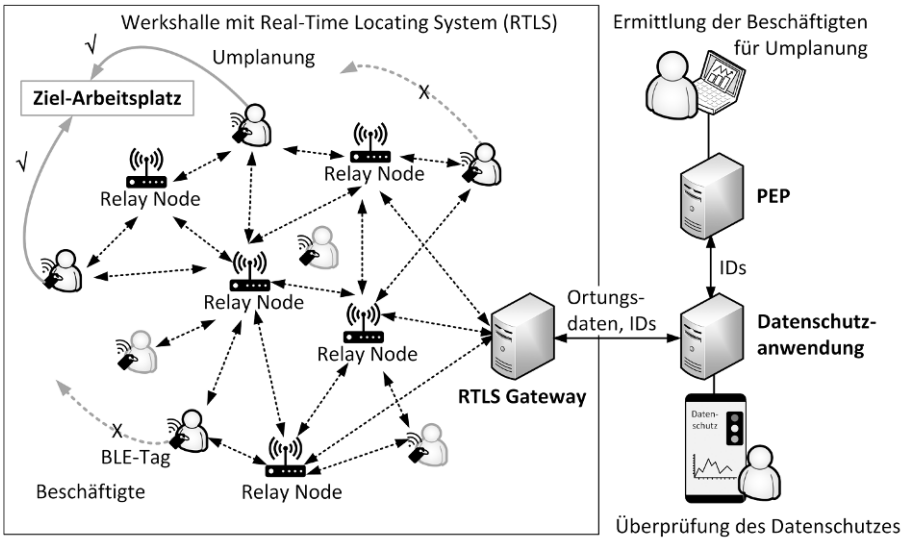
Die *Datenminimierung* (Art. 5 Abs. 1 lit. c DSGVO) besagt, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen. Die Erhebung der Standortdaten ist dann dem Zweck angemessen, wenn zum Zeitpunkt der Erhebung ein konkreter Bezug zur beabsichtigten Verwendung der Daten für die Personaleinsatzplanung besteht.[2] Erheblichkeit für den Zweck bedeutet, dass die erhobenen Daten dazu geeignet sein müssen, den mit der Datenverarbeitung verfolgten Zweck zu erreichen.[3] Dies bedeutet beispielsweise, dass die Beschäftigten, deren Standorte erhoben werden, nicht nur qualifiziert, sondern auch verfügbar sein müssen. Sind diese Beschäftigten gerade mit anderen Aufgaben beschäftigt, von denen sie nicht abgezogen werden können, dann wäre die Datenverarbeitung zwar angemessen, aber nicht erheblich. Beschränkt auf das notwendige Maß ist die Datenverarbeitung dann, wenn der ver-

2 Dies wäre beispielsweise dann nicht der Fall, wenn der Mitarbeiter aufgrund seiner Qualifikation offensichtlich nicht für den geplanten Einsatz geeignet ist.

3 *Schantz* in: BeckOK Datenschutzrecht [7], Art. 5 DS-GVO, Rn. 24; *Frenzel* in: Paal/Pauly [8], Art. 5 DSGVO, Rn. 35.

folgte Zweck ohne diese Datenverarbeitung nicht erreicht werden kann.[4] Bezogen auf die Standortbestimmung von Beschäftigten bedeutet dies, dass nur solche Daten erhoben werden dürfen, die für die Bestimmung der aktuellen Standorte von qualifizierten und verfügbaren Beschäftigten erforderlich sind. Die Erhebung weiterer Information, wie z. B. zur Arbeitsleistung oder dem Pausenverhalten, ist dagegen nicht erforderlich und damit nicht mit dem Datenminimierungsgebot vereinbar.

Abbildung 1 | Personaleinsatzplanung mit RTLS



Die *Speicherbegrenzung* (Art. 5 Abs. 1 lit. e DSGVO) besagt, dass personenbezogene Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Demnach müssen die Standortdaten der Beschäftigten gelöscht oder anonymisiert werden, wenn sie für den mit der Datenverarbeitung verfolgten Zweck (der Umplanung aufgrund eines besonderen Ereignisses) nicht länger benötigt werden.[5] Das Prinzip der Speicherbegrenzung ergänzt zum einen das Prinzip der Zweckbindung und konkretisiert zum anderen das Prinzip der Datenminimierung in zeitlicher Hinsicht.[6]

Darüber hinaus müssen die personenbezogenen Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet (*Integrität und Vertraulichkeit*, Art. 5 Abs. 1 lit. f DSGVO). Dies bedeutet insbesondere, dass der Zugriff auf die Standortdaten der Beschäftigten auf hierfür autorisierte Beschäftigte beschränkt werden muss, also z. B. Beschäftigte der Personaleinsatzplanung. Dies schließt ein, dass außerhalb des autorisierten Personenkreises die Daten grundsätzlich nicht weiterzugeben sind. Damit wird ebenfalls der Grundsatz der Datenminimierung gewahrt. Eine Ausnahme der Weitergabe besteht, wenn die Weiterverarbeitung der Daten zur Erreichung des vorgegebenen Zwecks erforderlich wird.[7]

4 Datenschutzfreundliche Umsetzung

Die oben beschriebenen Anwendungsszenarien werden im Forschungsprojekt *EduMiDa*[8] vom Anwendungspartner p.l.i. solutions[9], einem Anbieter von Personaleinsatzplanungslösungen, technisch umgesetzt und erprobt. Bei der technischen Umsetzung sind zahlreiche Anforderungen und Handlungsempfehlungen zu beachten (vgl. z. B. [4]). Diese betreffen u. a. die Möglichkeit einer Pseudonymisierung oder Anonymisierung, Zugriffsbeschränkungen auf die Ortungsdaten, die Vermeidung der Speicherung der Daten, die Verknüpfung der Daten mit anderen Systemen, die Vermeidung einer unnötig exakten Ortung sowie die Transparenz bzgl. der Verarbeitung der Daten. Grundsätzlich wurde bei der Umsetzung das Prinzip des *Privacy by Design* berücksichtigt, d. h., es werden nur so wenig personenbezogene Daten wie möglich verarbeitet.

4.1 Ermittlung von Standortdaten

Die in Abschnitt 2 beschriebenen Szenarien erfordern, den Standort von Beschäftigten auf dem Firmengelände und insbesondere innerhalb der Werks- und Lagerhallen zu bestimmen. Ortungssysteme, die nur im Freien funktionieren, wie etwa GPS, kommen daher nicht in Frage. Stattdessen kommt ein Echtzeit-Ortungssystem[10], das auf Bluetooth Low Energy (BLE) and Bluetooth Mesh basiert, zum Einsatz.[11] [12] Dazu ist in jeder Werkshalle ein Bluetooth Mesh installiert und mit einem zentralen RTLS-Gateway verbunden. Die Beschäftigten sind mit BLE-fähigen Geräten (einfache BLE-Tags oder auch vorhandene Smartphones) ausgestattet, die jeweils in periodischen Zeitabständen asynchrone Broadcast-Nachrichten („flooding“) senden. Innerhalb des BLE Mesh fungiert jeder Relay Node sowohl als Empfänger als auch als Sender und leitet jede Nachricht an jeden seiner Nachbarn weiter, außer zurück an die BLE-Tags, siehe Abbildung 1. So wird mit relativ wenigen Nodes eine große räumliche Abdeckung erreicht.

Die BLE-Tags haben jeweils eine eindeutige Kennung (ID) und sind genau einem Beschäftigten zugewiesen. Dadurch haben diese IDs den Charakter eines personenbezogenen Pseudonyms, dessen Auflösung nur im System der Personaleinsatzplanung möglich ist. Entsprechend sendet die PEP nur die IDs der für die Umplanung gesuchten Beschäftigten an das RTLS. Der Standort der betreffenden BLE-Tags wird anhand der Empfangssignalstärke (Received Signal Strength Indicator, RSSI) an jeweils drei oder mehr Nodes bestimmt, deren Position bekannt ist. Das RTLS-

4 Roßnagel in: Simitis/Hornung/Spiecker [9], Art. 5 Rn. 121.
5 Schantz in: BeckOK Datenschutzrecht [7], Art. 5 DS-GVO, Rn. 33.
6 Herbst in: [10], Art. 5 DS-GVO, Rn. 56, 65.
7 Außerhalb des Zwecks richtet sich die Weiterverarbeitung nach Art. 6 Abs. 4 DSGVO.
8 Projektseite EduMiDa: https://www.edumida.sit.fraunhofer.de/index.php
9 p.l.i. solutions GmbH, https://www.pli-solutions.de
10 Englisch: Real-Time Location System (RTLS)
11 Spezifikationen Mesh Model und Mesh Profile: https://www.bluetooth.com/specifications/specs/?types=specs-docs&keyword=mesh
12 Dennis Kwan: “Bluetooth Mesh profile applied to RTLS” (30.10.2017), https://www.bluetooth.com/blog/bluetooth-mesh-profile-applied-to-rtls/

Gateway berechnet die Ortungsdaten mittels Trilaterationsverfahren bis auf einen Meter genau und sendet über WLAN oder LAN die Daten an die Datenschutzanwendung. Dort wird ermittelt, welche Tags (d. h. welche gesuchten Beschäftigten) dem Ziel am nächsten sind. Die Anwendung antwortet dem PEP mit Angabe der entsprechenden IDs. Die Vorgänge werden protokolliert und in Form von Datenschutzmetriken zur Ansicht aufbereitet.

Durch den Einsatz des BLE-basierten Ortungssystems findet die Standortbestimmung der Beschäftigten per se nur auf dem Firmengelände statt und kann dort zudem auf bestimmte Bereiche beschränkt werden. Darüber hinaus werden die BLE-Tags als Wearables bereitgestellt, die die Beschäftigten ausschließlich auf dem Firmengelände tragen und beispielsweise während der Pausenzeiten ablegen können.

Die Verwendung des BLE-Netzes hat einige Vorteile gegenüber der alternativen Verwendung von WLAN- oder Ultrabreitband (UWB)-basierten RTLS-Systemen. Für Bluetooth Mesh sprechen vor allem der einfache, verbindungslose Protokoll-Stack, der geringe Stromverbrauch, die geringen Kosten und die breite Unterstützung von BLE in vielen Geräten. Anders als bei WLAN- oder UWB-Ortung, gibt es im Mesh-Protokoll für unberechtigte Dritte keine Möglichkeit, einzelne Tags zu identifizieren. Dies liegt vor allem daran, dass die Sicherheitsmechanismen in Bluetooth Mesh nicht optional sind, sondern aktiviert sein müssen.[13] Die Einrichtung eines BLE Mesh, das Hinzufügen oder Entfernen von Tags und das Verteilen von kryptografischen Schlüsseln erfolgt durch einen speziellen Node, den so genannten *Provisioner* und *Configuration Client*. Nutzdaten wie die übermittelten IDs werden sowohl auf der Netzwerkschicht als auch auf der Anwendungsschicht verschlüsselt, so dass kein Tracking möglich ist. Auch werden individuelle Geräteschlüssel vereinbart, die nur dem Node und dem Konfigurationsclient bekannt ist. Dadurch ist es z. B. möglich, in einen bestimmten Node die Schlüssel zu aktualisieren [3]. Der *Provisioner*-Node nimmt in der Regel nicht am Normalbetrieb teil. Auch wenn noch einige Forschungsfragen zu BLE Mesh offen sind [2], gilt das Bluetooth Mesh-Protokoll als relativ sicher, abgesehen von möglichen physischen Seitenkanalangriffen auf die AES-Schlüssel in der Hardware [1].

Als RTLS-System wird eine Middleware-Implementierung des RTLS-Industriestandards omlox[14] genutzt. Omlox ermöglicht die Vernetzung verschiedener Ortungstechnologien (RFID, SLAM, 5G, BLE, WLAN, GPS, optische Ortung, Ultraschallbasierte Ortung etc.), so dass Logistikkunden ein beliebiges, ggf. bereits vorhandenes RTLS weiter nutzen können. Die omlox-Middleware stellt alle Standortdaten über eine REST-API einheitlich in Form von GPS-Koordinaten bereit und unterstützt die Definition der Ortungsbereiche (Ziel-Arbeitsplätze, Sicherheitszonen etc.). Das RTLS-Gateway stellt die Ortungsdaten in Echtzeit bereit und überschreibt die jeweils vorigen Messdaten.

4.2 Verarbeitung der Standortdaten

Wie anhand der in Abschnitt 2 beschriebenen Szenarien erläutert, findet die Standortermittlung der Beschäftigten zum Zweck der agilen Personaleinsatzplanung statt: Im System der Personaleinsatzplanung (PEP) wird ein Technikausfall oder eine kurzfristige Mehrbelastung an einem Arbeitsplatz gemeldet, und es wird ermittelt, wie viele Beschäftigte mit einer bestimmten Qualifikation benötigt werden, um auf diese Ereignisse reagieren zu können. Die PEP sendet daraufhin eine Anfrage zur Erhebung von Standortdaten zusammen mit der benötigten Anzahl an Beschäftigten und den IDs der für das konkrete Ereignis qualifizierten Beschäftigten an die zentrale Datenschutzanwendung, die diese an das RTLS-Gateway weiterleitet, wo nun die Standorte der Beschäftigten anhand ihrer Tags ermittelt werden. Die Datenschutzanwendung bestimmt diejenigen Beschäftigten, die dem Ziel-Arbeitsplatz am nächsten sind und sendet deren IDs zurück an die PEP. Die eigentlichen Ortungsdaten werden dabei nicht übermittelt („Need-to-Know"-Prinzip). Die PEP kennt die Zuordnung der IDs zu den Beschäftigten und informiert die betreffenden Beschäftigten umgehend über die Umplanung. Die eigentlichen Ortungsdaten werden ausschließlich im RTLS-Gateway und in der Datenschutzanwendung verarbeitet und sind für die Protokollierung und Metrikenberechnung nicht mehr erforderlich. Sie werden daher nach erfolgter Umplanung gelöscht (d. h. keine dauerhafte Speicherung der Ortungsdaten). Zudem sind weder dem RTLS-Gateway noch der Datenschutzanwendung die Namen der Beschäftigten bekannt, sondern lediglich die IDs der BLE-Tags (Pseudonymisierung). Es findet keine Verknüpfung mit anderen personenbezogenen Daten statt. Die Datenschutzanwendung sorgt als eine Art Proxy für die Kontrolle der Anfragen und Zugriffe auf Ortungsdaten und dient damit den datenschutzrechtlichen Grundsätzen Datenminimierung und Speicherbegrenzung.

4.3 Kontrolle des Datenschutzes

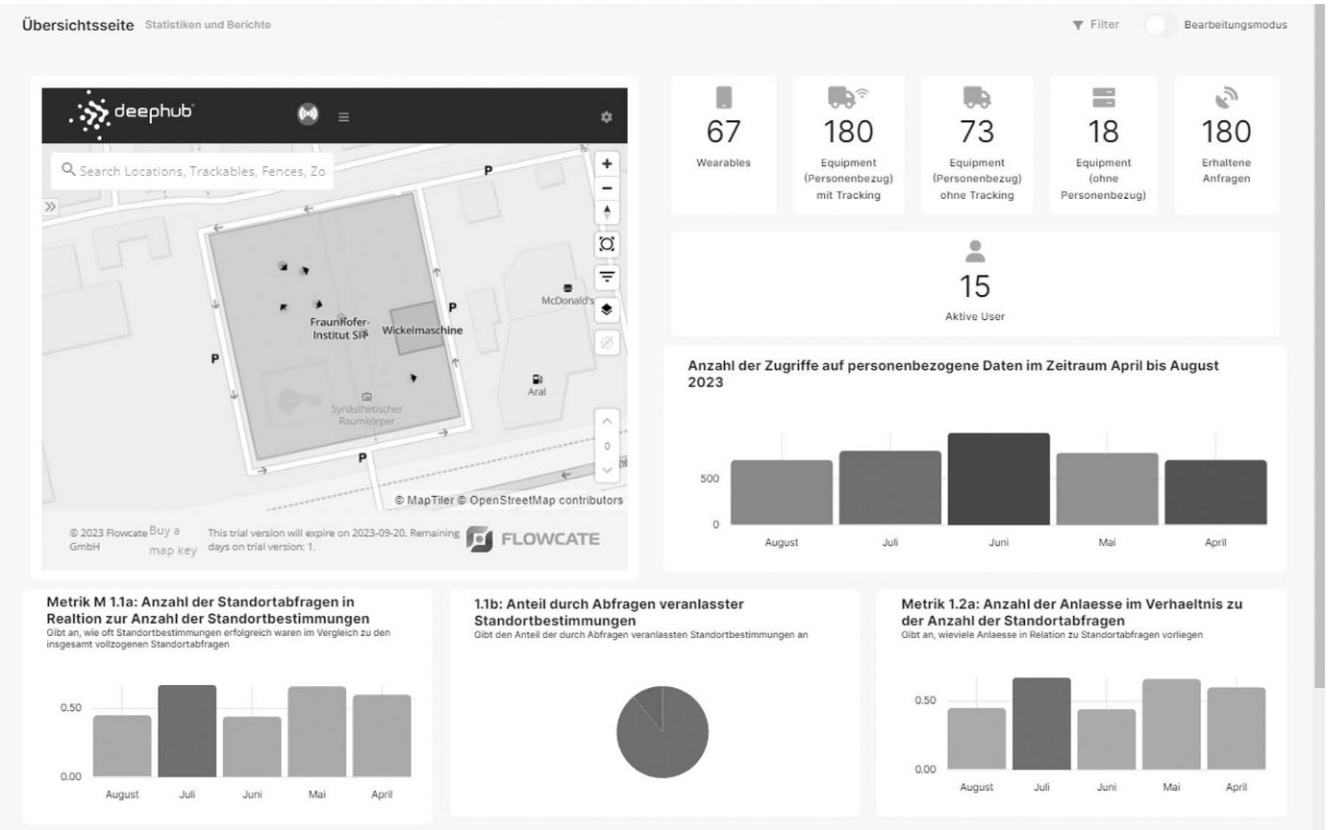
Typischerweise besteht in Unternehmen eine starke Abhängigkeit zwischen Arbeitgeber und den Arbeitnehmern. Daher ist es wichtig, neben der eigentlichen Umsetzung der Datenschutzanforderungen auch Kontrollmechanismen zu etablieren, mit deren Hilfe Datenschutzbeauftragte die Einhaltung der Datenschutzanforderungen verifizieren können.

Ein geeignetes Werkzeug für eine kontinuierliche und automatische Überwachung der Einhaltung der Datenschutzanforderungen stellen Datenschutzmetriken dar. Sie können helfen, die unrechtmäßige Erhebung und den Missbrauch personenbezogener Daten aufzudecken. Darüber hinaus ermöglichen es Metriken, den Grad der Umsetzung von Datenschutzzielen wie Datenminimierung oder Speicherbegrenzung zu untersuchen. Um die abstrakten Datenschutzanforderungen der DSGVO umzusetzen, müssen diese in konkrete (technische) Maßnahmen übersetzt werden (vgl. Abschnitt 4.2). Den Grad der Umsetzung dieser Maßnahmen lässt sich wiederum mithilfe der Metriken überprüfen. Um aussagekräftige Ergebnisse zu erzielen, müssen Metriken auf Eigenschaften beruhen, die für das Datenschutzziel relevant und quantifizierbar sind [11]. Um Messgrößen zur Bestimmung des Umsetzungsgrades der Datenschutzziele zu definieren, ist es daher notwendig, tatsächlich verfügbare und geeignete Messdaten zu identifizieren, in unseren Szenarien unter anderem die Häufigkeit von Standortermittlungen und die Zahl der Beschäftigten, deren Standort ermittelt wurde. Idealerweise liefern solche Metriken als Ergebnis Kennzahlen in Form einer Prozentzahl oder einer reellen Zahl zwischen 0 und 1. Ein Wert von 0 oder 0% deutet darauf hin, dass die mit der Metrik zu überprüfende Maßnahme gar nicht umgesetzt wurde oder es einen er-

13 Kai Ren, Martin Woolley: Bluetooth Mesh Security Overview (11.9.2017), https://www.bluetooth.com/blog/bluetooth-mesh-security-overview/

14 Omlox, The open locating standard, https://omlox.com/

Abbildung 2: Metriken-Dashboard



heblichen Datenmissbrauch gibt, während 1 bzw. 100% bedeutet, dass die Maßnahme korrekt umgesetzt wurde und es keinen Datenmissbrauch zu geben scheint.

In [5] und [6] haben die Autoren einige konkrete Datenschutzmetriken entwickelt, die dazu beitragen, die Umsetzung der Datenschutzziele Datenminimierung und Speicherbegrenzung zu überprüfen. Mithilfe dieser Metriken lässt sich unter anderem verifizieren, ob die Standortermittlungen auf Fälle beschränkt sind, in denen ein konkreter Anlass vorliegt (z. B. ein Technikausfall), und ob die Ermittlung von Standorten von Beschäftigten, die nicht für ein bestimmtes Ereignis in Frage kommen, unterlassen wurde (Datenminimierung). Weiterhin lässt sich mit diesen Metriken verifizieren, ob nach Beendigung eines Ereignisses, wie der Umplanung von Beschäftigten aufgrund einer kurzfristigen Mehrbelastung, die dazu erhobenen Standortdaten von Beschäftigten gelöscht wurden (Speicherbegrenzung).

4.4 Transparenz durch Dashboard

Um die Kontrolle des Datenschutzes zu ermöglichen, wurde ein Dashboard entwickelt, auf dem die auf Basis der im vorherigen Abschnitt erläuterten Metriken berechneten Kennzahlen in Form von Diagrammen angezeigt werden (Abbildung 2). Auf diese Weise kann z. B. ein Datenschutzbeauftragter auf einen Blick erkennen, ob es Hinweise auf Datenmissbrauch oder Probleme bei der Umsetzung von Datenschutzmaßnahmen gibt.

Dieses Dashboard wurde zudem um eine spezielle Anzeige für die einzelnen Beschäftigten im Employee Self Service (ESS) erweitert. Dies ermöglicht es den betroffenen Beschäftigten, die über sie erhobenen Daten einzusehen. In einer tabellarischen Übersicht sehen die Beschäftigten, zu welchen Zeitpunkten ihr aktueller Standort erhoben wurde und zu welchem Zweck. Unterstützt wird diese Darstellung um Diagramme, mit deren Hilfe die Beschäftigten sehr schnell erkennen können, wie oft in welchen Zeiträumen ihr Standort erhoben wurde. Auf diese Weise werden die Beschäftigten in die Lage versetzt, die Verarbeitung ihrer Standortdaten nachvollziehen zu können. Das Dashboard im ESS fördert somit die Transparenz im Sinne des Art. 5 Abs. 1 Var. 2 DSGVO bzgl. der Verarbeitung der Standortdaten von Beschäftigten (vgl. auch [12]).

5 Fazit

Der Beitrag hat gezeigt, wie Szenarien aus dem Bereich der Intralogistik, in denen eine Live-Ortung von Beschäftigten erforderlich ist, datenschutzfreundlich gestaltet werden können und wie die hohen Anforderungen der DSGVO an die Rechtmäßigkeit der Datenverarbeitung durch das Unternehmen in der Praxis umgesetzt werden können. Insbesondere die Bereitstellung des im Abschnitt 4.4 beschriebenen Dashboards trägt zur Etablierung eines technologiegestützten Beschäftigtendatenschutzes bei und steigert die Transparenz der Datenverarbeitung. Denn Dashboards bieten eine Möglichkeit, gebündelt und anschaulich Informationen zur Datenverarbeitung durch das Unternehmen den Mitarbeitenden zur Verfügung zu stellen. Die Mitarbeitenden werden damit in die Lage versetzt, die Datenverarbeitungen kontrollieren und auf diese reagieren zu können, insbesondere

wird ihnen dadurch die Wahrnehmung der ihnen zustehenden (Betroffenen-)Rechte ermöglicht.[15] Dashboards können außerdem dazu verwendet werden, eine komfortable Plattform für die Durchsetzung dieser Betroffenenrechte durch die Mitarbeitenden zu schaffen. Die transparente Darstellung der Datenverarbeitungen auf einem Dashboard ist folglich ein wichtiger Schritt, um dem Beschäftigten die Ausübung seines Rechts auf informationelle Selbstbestimmung zu gewährleisten.[16] So profitieren im Ergebnis sowohl das Unternehmen als auch die Mitarbeitenden von einer datenschutzfreundlichen Implementierung.

Zu beachten ist, dass für eine datenschutzfreundliche Ausgestaltung der in diesem Beitrag dargestellten Szenarien neben den beschriebenen technischen Maßnahmen auch einige organisatorische Maßnahmen umzusetzen sind. Hierzu zählt u. a., dass die Beschäftigten vorab auf verständliche Weise über die Live-Ortung, deren Zweck und Funktionsweise informiert werden (z. B. durch Informationsveranstaltungen und -broschüren) und dass der Betriebsrat bei der Umsetzung der Live-Ortung involviert wird.

Literatur

[1] Adomnicai, A.; Fournier, J. J.A.; Masson, L.: Hardware security threats against Bluetooth mesh networks. IEEE Conference on Communications and Network Security (CNS), 2018.

[2] Barua, A.; Al Alamin, M. A.; Hossain, M. S.; Hossain, E.: Security and privacy threats for bluetooth low energy in IoT and wearable devices: A comprehensive survey. IEEE Open Journal of the Communications Society, Vol. 3, 2022.

[3] Caesar, M.; Steffan, J.: A location privacy analysis of bluetooth mesh. Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019.

[4] Conrad, C. S.: Datenschutz bei Live-Ortung & GPS-Tracking von Beschäftigten. Datenschutz und Datensicherheit, Vol. 47, 2023.

[5] Schleper, J.; Kohn, M.; Pesch, P. J.; Waldmann, U.; Kunz, T.: Messung der Datenminimierung für den Beschäftigtendatenschutz am Beispiel von Standortdaten. INFORMATIK 2022, Gesellschaft für Informatik, Bonn, 2022.

[6] Waldmann, U.; Kunz, T.; Schleper, J.; Kohn, M.; Pesch, P. J.: Legal Requirements and Technical Metrics for Controlling Privacy of Employees' Location Data. Mensch und Computer 2023 – 9. Usable Security und Privacy Workshop, 2023.

[7] Wolff, H. A.; Brink, S.: Beck'scher Online-Kommentar Datenschutzrecht. 39. Edition, Stand: 01.02.2022.

[8] Paal, B; Pauly, D. A. (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz – DS-GVO BDSG. 3. Aufl. 2021.

[9] Simitis, S.; Hornung, G.; Spiecker gen. Döhmann, I. (Hrsg.): Datenschutzrecht – DSGVO mit BDSG. 2019.

[10] Kühling, J.; Buchner, B. (Eds.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. C.H. BECK, München. 2024.

[11] Böhme, R.; Freiling, F. C. 2008. On Metrics and Measurements. Springer, Berlin, Heidelberg, 2008.

[12] Tolsdorf, J.; Bosse, C. K.; Dietrich, A.; Feth, D.; Schmitt, H.: Privatheit am Arbeitsplatz. Datenschutz und Datensicherheit, Vol. 44, 2020.

15 Herbst in: [10], Art. 5 DS-GVO, Rn. 18.

16 Ebd.