Messung der Datenminimierung für den Beschäftigtendatenschutz am Beispiel von Standortdaten

Verifikation der datenschutzrechtlichen Anforderungen an die Datenminimierung mithilfe von Metriken[1]

Janine Schleper[2], Matthias Kohn[3], Paulina Jo Pesch[4], Ulrich Waldmann[5], Thomas Kunz[6]

Abstract: Metriken zur automatisierten Verifizierung der Umsetzung des Datenminimierungsgebots können Unternehmen darin unterstützen, ihren Kontrollpflichten nachzukommen und das Vertrauen ihrer Beschäftigten in eine datenschutzkonforme Verarbeitung ihrer Daten zu stärken. Um sich durch eine Metrik einer komplexen datenschutzrechtlichen Anforderung wie dem Gebot der Datenminimierung anzunähern, sind geeignete Datenquellen sinnvoll miteinander zu kombinieren. Diese Arbeit skizziert grundlegende Metriken zur Kontrolle der Datenminimierung anhand eines Anwendungsszenarios im Bereich der agilen Personaleinsatzplanung und beschreibt die prototypische Umsetzung dieser Metriken.

Keywords: Automatisierte Kontrolle; Datenschutz; Messquellen; Metrik; Datenminimierung

1 Herausforderungen und Ziel

Metriken bieten die Möglichkeit, den Grad der Umsetzung von Datenschutzvorschriften wie dem Datenminimierungsgebot auf Grundlage von Messdaten automatisiert zu verifizieren. Sie können Unternehmen dabei unterstützen, von mehreren Optionen die datenschutzfreundlichste zu ermitteln oder über die Einhaltung von Datenschutzvorschriften Rechenschaft abzulegen – und dies sowohl gegenüber Aufsichtsbehörden und betrieblichen

[1] Das diesem Beitrag zugrunde liegende Vorhaben EduMiDa wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 16KIS1361K, 16KIS1362 und 16KIS1363 gefördert. Die Verantwortung für den Inhalt liegt bei den Autor*innen. Michael Koddebusch gebührt unser Dank für hilfreiche Hinweise.

[2] Universität Bremen, Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universitätsallee, 28359 Bremen, Deutschland, schleper@uni-bremen.de

[3] Universität Bremen, Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universitätsallee, 28359 Bremen, Deutschland, kohn@uni-bremen.de

[4] WWU Münster, Institut für Wirtschaftsinformatik, Leonardo-Campus 3, 48149 Münster, Deutschland, paulina.pesch@uni-muenster.de

[5] Fraunhofer SIT, Cloud Computing, Identity Privacy (CIP), Rheinstr. 75, 64295 Darmstadt, Deutschland, ulrich.waldmann@sit.fraunhofer.de

[6] Fraunhofer SIT, Cloud Computing, Identity Privacy (CIP), Rheinstr. 75, 64295 Darmstadt, Deutschland, thomas.kunz@sit.fraunhofer.de

doi:10.18420/inf2022_21

Datenschutzbeauftragten, als auch gegenüber Betroffenen. Gerade für die Verbesserung und Kontrolle des Beschäftigtendatenschutzes durch Unternehmen bieten sich Metriken an [3]. Dies gilt insb. für das in Art. 5 Abs. 1 lit. c DSGVO verankerte Datenminimierungsgebot (im Einzelnen s. Abschnitt 2). Unternehmen, die entgegen der Vorschrift zu viele Daten verarbeiten, drohen gemäß Art. 83 Abs. 5 lit. a DSGVO hohe Bußgelder.

2 Anwendungsszenario und Anforderungen

In der Logistikbranche verspricht die Nutzung von Echtzeit-Standortdaten wirtschaftliche Vorteile. So kann zur Aufrechterhaltung des Betriebsablaufs eine agile Personaleinsatzplanung (PEP) erforderlich sein und die Nutzung von Standortdaten Kosten senken. Wenn auf einem großen Betriebsgelände eine technische Anlage ausfällt, müssen nicht nur Beschäftigte ermittelt werden, die qualifiziert sind die Anlage zu reparieren und sich im Dienst befinden, sondern ist auch die Identifikation der Beschäftigten sinnvoll, die die Anlage möglichst schnell erreichen können. So können Beschäftigte eingesetzt werden, für deren Einsatzortverlegung möglichst geringe Kosten anfallen. Die Verarbeitung von Standorten muss dem Datenminierungsgebot nach Art. 5 Abs. 1 lit. c DSGVO genügen. Danach müssen personenbezogene Daten dem Zweck *angemessen* und *erheblich* sowie auf das für die Zwecke der Verarbeitung *notwendige Maß* beschränkt sein. Dies erfordert eine möglichst weitgehende Begrenzung der Verarbeitung personenbezogener Daten sowohl im Hinblick auf Quantität, als auch auf Qualität.[7]

Die Datenverarbeitung ist dem Zweck *angemessen*, wenn ein objektiver sachlicher Bezug hinsichtlich Funktion, Inhalt und Umfang zum damit verfolgten Zweck vorliegt.[8] Die Erhebung der Standortdaten muss also zum Zeitpunkt der Datenabfrage in konkretem Bezug zur Beschäftigteneinsatzplanung stehen. Das wäre nicht der Fall, wenn der Beschäftigte für die geplante Tätigkeit erkennbar nicht geeignet ist, etwa eine Reinigungskraft für die Reparatur einer Industrieanlage.

Erheblichkeit für den Zweck setzt voraus, dass die erhobenen Daten objektiv dazu geeignet sind, den mit der Datenverarbeitung verfolgten Zweck zu erreichen.[9] Dafür müssen die erhobenen Daten zumindest für einen Teilaspekt des verfolgten Zwecks bedeutend sein und dessen Erreichung dienen.[10] Die Erhebung des Standorts einer Person, die für die vorgesehene Aufgabe zwar qualifiziert ist, der aber gerade keine dienstliche Anweisung erteilt werden kann, ist zwar angemessen, jedoch nicht erheblich.

Beschränkt auf das *notwendige Maß* ist die Datenverarbeitung dann nicht mehr, wenn der verfolgte Zweck auch ohne die Datenverarbeitung erreicht werden kann.[11] Es sind nur

[7] *Frenzel* in: [6], Art. 5 DSGVO, Rn. 34.
[8] *Herbst* in: [5], Art. 5 DSGVO, Rn. 57; *Roßnagel* in: [7], Art. 5 Rn. 119.
[9] *Schantz* in: [8], Art. 5 DS-GVO, Rn. 24; *Frenzel* in: [6], Art. 5 DSGVO, Rn. 35.
[10] *Roßnagel* in: [7], Art. 5 Rn. 120.
[11] *Roßnagel* in: [7], Art. 5 Rn. 121.

solche Daten zu erheben, die zur Bestimmung des aktuellen Standorts der qualifizierten, diensthabenden Beschäftigten auf dem Werksgelände notwendig sind, um die Person ausfindig zu machen, die die Anweisung zur Reparatur der Anlage erhalten soll. Dies erfordert nicht die Nutzung von Standortdaten zur Ermittlung weiterer Informationen wie etwa zur Arbeitsleistung, Körperhaltung, Bewegung, zum Verhalten in den Pausen oder dem Gesundheitszustand der Beschäftigten, sodass eine Erhebung dieser Daten nicht notwendig und damit nicht mit dem Datenminimierungsgebot vereinbar wäre.

3 Metrikenentwicklung und Messpunkte

Überprüfen lässt sich der Grad der Einhaltung des Datenminimierungsgebots durch Metriken, d. h. präzise definierte Methoden zur Messung bestimmter Attribute eines (Teil-)Systems [2]. **Datenschutzmetriken** dienen speziell der Messung des Grades der Umsetzung datenschutzrechtlicher Ziele wie z. B. Datensicherheit oder Datensparsamkeit. Unternehmen können sich solcher Metriken bedienen, um bei der Wahl zwischen mehreren Lösungen oder der Konfiguration der von ihnen eingesetzten Software die datenschutzfreundlichste Option zu ermitteln oder um Aufsichtsbehörden und Betroffenen gegenüber ein hohes Datenschutzniveau zu demonstrieren.

Einerseits lassen sich Metriken *„bottom up“* ausgehend von den tatsächlich verfügbaren Messdaten entwickeln [1]. Bei Datenschutzmetriken, mittels derer Unternehmen eigene Systeme überprüfen und die eigene Compliance nachweisen, können – anders als bei Metriken zur Überprüfung der Compliance Dritter wie z. B. Cloud-Anbieter [4] – Daten direkt im System erhoben und Messverfahren in dieses implementiert werden. Andererseits lassen sich Metriken *„top down“* ausgehend von dem Ziel entwickeln, für das der Grad der Umsetzung durch die Metrik ermittelt werden soll [1]. Für Datenschutzmetriken besteht dieses in der jeweilig überprüften datenschutzrechtlichen Anforderung, z. B. Datensicherheit oder Datenminimierung. Dabei sind in einem ersten Schritt aus der unspezifischen, abstrakten datenschutzrechtlichen Anforderung konkrete Maßnahmen abzuleiten [4] und dann Metriken zur Messung des Grades der Umsetzung der Maßnahmen zu bilden.

Metriken lassen sich *„top down“* ausgehend von den in Abschnitt 2 beschriebenen einzelnen **Anforderungen** des Datenminimierungsgebots ableiten: Die Daten müssen einen objektiv-sachlichen Bezug zum Verarbeitungszweck aufweisen (Angemessenheit) und ihre Verarbeitung muss zur Zweckerreichung geeignet sein (Erheblichkeit) und auf das notwendige Maß beschränkt sein.

Hieraus lassen sich Maßnahmen entwickeln, deren Einhaltung messbar ist. Das Datenminimierungsgebot misst Anforderungen an die Datenverarbeitung an ihrem Zweck bzw. Anlass. Deshalb lässt sich bloß auf Grundlage der Häufigkeit oder des Umfangs von Datenabfragen kaum eine Aussage darüber treffen, inwieweit dem Gebot der Datenminimierung genüge getan worden ist. Selbst eine einzige Datenabfrage geringen Umfangs kann dem Gebot der Datenminimierung zuwiderlaufen oder eine Vielzahl umfangreicher Datenabfragen

kann mit ihm zu vereinbaren sein. Für das Anwendungsszenario ergeben sich folgende, zu kombinierende **Maßnahmen**:

1. Anlasslose Standortbestimmungen sind zu unterlassen. Hierzu sind zwei Maßnahmen umzusetzen: Standortbestimmungen dürfen (a) nur im Fall einer Standortabfrage und (b) nur bei konkretem Anlass stattfinden.
2. Es dürfen nur Standorte für den konkreten Einsatz in Betracht kommender Beschäftigter bestimmt werden.

Für eine Metrik zur Kontrolle der Datenminimierung bei Standortabfragen sind zur Ermittlung des Umfangs der Datenverarbeitung als **Indikatoren** insb. Metadaten von Abfragen (Zeitstempel, Spezifikation, z. B. durch Filter wie Qualifikation und Zeitraum des Einsatzes), Metadaten ermittelter Standorte wie insb. die Zahl der Betroffenen sowie Daten zu den Betroffenen heranzuziehen. Daneben lässt sich aus Personallisten, Berufsbezeichnungen und Qualifikationen sowie Dienstplänen und Abwesenheitsvermerken schließen, welche Beschäftigten wann für welche Einsätze in Betracht kommen. Ggfs. erlauben die Betriebsabläufe auch die Erhebung von Daten, die indizieren, ob Anlass zur Standortdatenerhebung besteht, z. B. durch in Anlagen verbaute Sensoren.

Um zu überprüfen, dass Standorte nur auf Abfragen hin ermittelt werden, schlagen wir folgende **Metrik 1a** vor, die für einen bestimmten Zeitraum den Anteil durch Abfragen veranlasster Standortbestimmungen (*AvS(Zeitraum)*) bestimmt:

$$\text{AvS(Zeitraum)} = \frac{\text{Zahl Standortabfragen}}{\text{Zahl Standortbestimmungen}} \tag{1a}$$

Wir verwenden den Begriff der Standortbestimmung für die Berechnung eines oder mehrerer Standorte in einem Zusammenhang, wobei wir durch dieselbe Abfrage veranlasste Standortberechnungen als eine Standortbestimmung werten. Ziel ist es, dass die Zahl der Standortabfragen der Zahl der Standortbestimmungen entspricht, Zielwert ist dementsprechend 1. Unter 1 liegende Werte sagen aus, dass mehr Standortbestimmungen stattgefunden haben als aufgrund von Abfragen geboten. Je weiter sich die Kennzahl 0 annähert, umso mehr Standortbestimmungen haben ohne Anfrage und damit anlasslos stattgefunden.

Die Unterlassung anlassloser Standortabfragen lässt sich durch **Metrik 1b** verifizieren, wenn Daten über Anlagenausfälle und erhöhten Personalbedarf verfügbar sind. Metrik 1b bestimmt für einen gegebenen Zeitraum den Anteil der real veranlassten Abfragen für eine standortbasierte Einsatzplanung von der Gesamtzahl der Standortabfragen (*ArA(Zeitraum)*), Zielwert ist wiederum 1:

$$\text{ArA(Zeitraum)} = \frac{\text{Zahl Anlässe}}{\text{Zahl Standortabfragen}} \tag{1b}$$

Die Unterlassung der Erhebung von Standorten Beschäftigter, die nicht für einen Einsatz in Frage kommen, lässt sich durch folgende **Metrik 2** verifizieren, die für eine bestimmte Abfrage die Anzahl der ermittelten Standorte zur Anzahl der für einen Einsatz in Betracht kommenden Beschäftigten setzt (Anteil anlassbezogener Standorte *AaS*), Zielwert ist wiederum 1:

$$\text{AaS} = \frac{\text{Zahl in Betracht kommender Beschäftigten}}{\text{Zahl ermittelter Standorte}} \tag{2}$$

4 Beispielhafte Umsetzung der Metriken

Eine beispielhafte Architektur zur Umsetzung des Metrikensystems veranschaulicht Abb. 1. Das Metrikensystem ist eine unabhängige und vertrauenswürdige Komponente innerhalb des Unternehmensnetzwerks mit klar definierten und beschränkten Zugriffsrechten und Benutzungsschnittstellen.

Die Beschäftigten tragen aktive Wearables am Körper und diese funken ihre technischen Kennungen an die in den Werkshallen verteilten Empfänger, die die gemessenen Signalübertragungszeiten und Kennungen an ein Gateway senden. Das Gateway berechnet in Echtzeit aus den Signallaufzeiten die Positionsdaten der Wearables und damit der Beschäftigten. Die Standorte werden vom PEP-Tool abgefragt und den Beschäftigten zugeordnet. Das Gateway protokolliert die Häufigkeit der Standortbestimmungen, die Zahl der Standortabfragen sowie die Zahl der gemessenen Standorte mit den zugehörigen Zeitpunkten und hält die Daten für einen gewissen Zeitraum vor. Im PEP-Tool werden die Anlässe für die Umplanung von Beschäftigten wie auch die jeweils in Betracht kommenden Beschäftigten hinterlegt. Dazu müssen im PEP-Tool Informationen über Maschinenausfälle, erhöhten Personalbedarf und Katastrophenfälle automatisch durch andere Systeme oder manuell eingetragen werden.

Das Metrikensytem ruft regelmäßig diese Daten vom Gateway und dem PEP-Tool ab, um die Metriken zu berechnen. Die Endgeräte, Infrastrukturkomponenten und weiteren technischen Komponenten müssen für ihre Nutzung im Rahmen des Metrikensystems zwar bestimmte Funktionen und Schnittstellen unterstützen, sind aber nicht auf herstellerspezifische Produkte beschränkt. Anhand der Metriken können z. B. der Betriebsrat, Datenschutzbeauftragte oder auch die Betroffenen selbst den Beschäftigtendatenschutz innerhalb des Unternehmens überwachen.

5 Diskussion und Ausblick

Die *Metriken sind weiterzuentwickeln und zu evaluieren*. Die vorgeschlagenen Metriken beschränken sich auf die Bestimmung von Anteilen. Um ihre Aussagekraft zu erhöhen, ist die Einbeziehung weiterer Daten, wie Zeitstempel und Pseudonyme in Betracht zu ziehen.

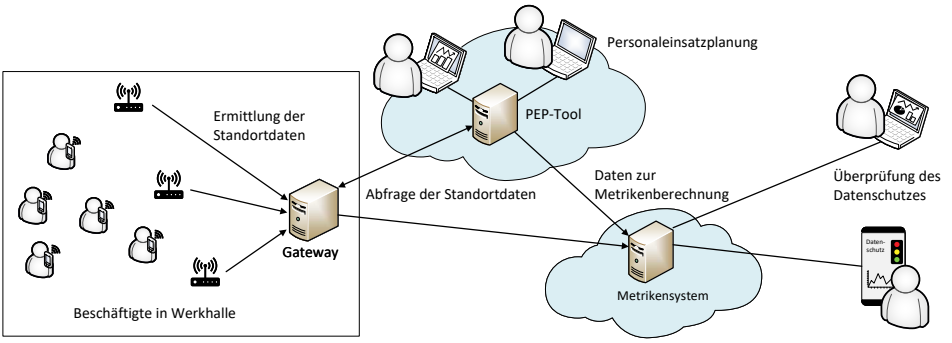

Abb. 1: Beispiel-Architektur des Metrikensystems

Notwendig ist die *Entwicklung weiterer Metriken* zur Kontrolle der Datenminimierung, etwa für andere Anwendungsszenarien. Auch ließe sich eine komplexere Metrik formulieren, mittels derer sich mehrere PEP-Lösungen unter Datensparsamkeits- und Effizienzgesichtspunkten miteinander vergleichen lassen. Dabei wäre der Umfang der mit der PEP-Lösung verbundenen Datenverarbeitungsvorgänge in Beziehung zu den durch sie zu vermeidenden Fehlern und Schwächen der Personalplanung zu setzen. Hierdurch ließe sich validieren, ob die Nutzung von Standortdaten für die agile Einsatzplanung für ein Unternehmen überhaupt erforderlich ist. Weiterhin bedarf es für einen starken, verifizierbaren Beschäftigtendatenschutz weiterer Datenschutzmetriken zur Kontrolle auch anderer Anforderungen des Datenschutzrechts wie etwa Datensicherheit und Speicherbegrenzung.

Literaturverzeichnis

[1] Ammann, F.-E.; Sowa, A.: „Systematische Entwicklung von Metriken zur Beurteilung der Datensicherheit“. Datenschutz und Datensicherheit (DuD) 4/2012, 247–252.

[2] Böhme, R.; Freiling , F. C.: „On Metrics and Measurements“. In: Eusgeld, I.; Freiling, F. C.; Reussner, R. (Hrsg.). „Dependability Metrics“. 2008.

[3] Diel, S.; Kohn, M.; Schleper, J.; Selzer, A.: „Datenschutzmetriken im Beschäftigungsverhältnis“. DuD 12/2021.

[4] Jäger, B.; Selzer, A.; Waldmann. U.: „Die automatisierte Messung von Cloud-Verarbeitungsstandorten“. DuD 1/2015.

[5] Kühling, J.; Buchner, B. (Hrsg.): „DS-GVO / BDSG“. 3. Aufl. 2020.

[6] Paal, B; Pauly, D. A. (Hrsg.): „DS-GVO BDSG“. 3. Aufl. 2021.

[7] Simitis, S.; Hornung, G.; Spiecker gen. Döhmann, I. (Hrsg.): „Datenschutzrecht“. 2019.

[8] Wolff, H. A.; Brink, S.: „BeckOK Datenschutzrecht“. 39. Edition, Stand: 01.02.2022.