

EIN INSTRUMENT ZUR BEWERTUNG DER AUSWIRKUNGEN AUF DIE PRIVATSPHÄRE AUFGRUND DER DATENVERARBEITUNG IM INTERNET DER DINGE (IOT)

Tobias Mettler, Dana Naous
4th Juli 2023



In Zusammen-
Arbeit mit:

 **IDHEAP**
POLICY BRIEF

EINLEITUNG

Die Datenschutz-Grundverordnung der EU (DSGVO) hat die Datenschutz-Folgenabschätzung (DSFA) als Instrument zur Bewertung der Risiken eingeführt, die mit der Technologie und der Verarbeitung von Daten für die Privatsphäre verbunden sind. Die DSFA zielt also darauf ab, die Risiken von Schäden für natürliche Personen zu identifizieren und zu reduzieren. Um dies zu erreichen, wird die DSFA immer dann durchgeführt, wenn eine hohe Wahrscheinlichkeit besteht, dass die Datenverarbeitung zu Risiken für die Rechte und Freiheiten der betreffenden Personen führen kann. Diese Art von Bewertung ermöglicht es nicht nur, die Einhaltung der Gesetze zu messen, sondern auch sicherzustellen, dass Datenschutzfragen von Anfang an bei der Entwicklung und Nutzung von Informationstechnologien berücksichtigt werden.

So ermöglicht die DSFA den Datenverwalter:innen, die negativen Auswirkungen von Datenverarbeitungstechnologien auf Einzelpersonen zu erkennen, zu behandeln und abzuschwächen. Da die gesetzliche Bestimmung der DSGVO jedoch abstrakt ist, wird die Durchführung solcher Bewertungen häufig als subjektiv kritisiert (Wagner und Boiten 2018). Daher ist es notwendig, konkrete und detaillierte Richtlinien in den Bewertungsprozess einzuführen sowie automatisierte Tools, die die Analyse beschleunigen können.

FORSCHUNGSANSATZ

Um die Methodik zur Bewertung von Datenschutzrisiken zu verbessern, haben wir ein praktisches Werkzeug entwickelt, das es Organisationen ermöglicht, objektivere Bewertungen vorzunehmen. Da diese Art der Bewertung je nach Einsatzbereich variiert, behandeln wir ein spezielles Szenario der Verarbeitung von Daten aus dem Internet der Dinge (IoT) in der vernetzten Überwachung. IoT-Initiativen mit tragbaren Geräten und Sensornetzen ermöglichen den Zugriff auf verschiedene Arten von Daten. Sie werden in Organisationen für die digitale Überwachung vor allem eingesetzt, um Gesundheitsprobleme zu erkennen und zu verhindern und um Gesundheitsrisiken zu mindern. Ihre Verwendung ist jedoch mit Risiken für die Privatsphäre verbunden. Wir möchten einen Beitrag zur Diskussion über die Umsetzung der DSFA leisten, indem wir Datenkontrolleur:innen praktische Hilfe in Form eines automatisierten DSFA-Tools für IoT-Projekte anbieten. Im Rahmen eines kontinuierlichen Risikomanagementansatzes schlagen wir einen strukturierten Bewertungsprozess vor, der mehrere Phasen umfasst. In der ersten Phase beantwortet das Tool Fragen zum Ziel des Projekts, zum Kontext und zur Art der Datenverarbeitung. Die zweite Phase umfasst detaillierte Fragen zur Analyse des Datenflusses, d. h. zur Sammlung, Speicherung und Nutzung von Daten. In dieser Phase werden auch die verschiedenen Rollen ermittelt, um die unterschiedlichen Personen zu dokumentieren, die in den Prozess involviert sind. Die dritte Phase besteht aus einer Datenschutzanalyse, bei der die Risiken für die Privatsphäre anhand einer Reihe relevanter Fragen ermittelt und im Hinblick auf die Grundsätze des Datenschutzes bewertet werden. Die letzte Phase beinhaltet die Dokumentation und Visualisierung der Ergebnisse in einem Bericht, in dem die Auswirkungen auf die Privatsphäre analysiert werden.

ABBILDUNG 1 | VERFAHREN ZUR BEWERTUNG DES RISIKOS FÜR DIE PRIVATSPHÄRE IN DEM VON UNS ENTWICKELTEN TOOL



ERGEBNISSE, DISKUSSIONSGRUNDLAGE UND IMPLIKATIONEN FÜR ENTSCHEIDUNGSTRÄGER:INNEN

Das entwickelte Tool bietet Ratschläge zum DSFA-Prozess und dokumentiert die Ergebnisse, damit Datenkontrolleur:innen die Risiken, die sich aus der Nutzung der IoT-Technologie ergeben, erkennen und angehen können. Darüber hinaus bieten wir mithilfe der Checkliste eine Bestätigungsanalyse des Implementierungsprozesses und der Verfügbarkeit spezieller Garantien zur Wahrung der Vertraulichkeit von Daten. Obwohl dieses Tool speziell für den Kontext der vernetzten Überwachung entwickelt wurde, kann sein Anwendungsbereich noch auf andere Technologien wie KI-Systeme mit algorithmischem Management und auf andere Umgebungen als den Gesundheitsbereich ausgeweitet werden. Für unsere künftige Forschung wird das Tool von Praktiker:innen evaluiert, um mögliche Erweiterungen vorschlagen zu können. Wir möchten das Tool auch mit Nutzer:innen testen, um die Rolle des «Privacy Priming» zu bewerten, d. h. über das Tool Informationen über die Risiken für die Privatsphäre und die Akzeptanz von vernetzter Technologie am Arbeitsplatz zu erhalten.

Bemerkung: Dieser Artikel wurde im Rahmen des [IDHEAP Policy Brief No. 6](#) veröffentlicht.

Referenzen:

- Mettler, T., & Naous, D. (2022). Beyond Panoptic Surveillance: On the Ethical Dilemmas of the Connected Workplace. In: European Conference on Information Systems (ECIS). Timisoara, Romania

- Wagner, I. & Boiten, E. (2018). Privacy Risk Assessment: From Art to Science, by Metrics. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp. 225-241: Springer.

Bild: unsplash.com