Gesamtvorhabenbeschreibung

(zur vertraulichen Behandlung)

EMPRI-DEVOPS

Employee Privacy in Software Development and Operations

Verbundkoordinator:
Prof. Dr.-Ing. Hannes Federrath
Universität Hamburg, FB Informatik
Vogt-Kölln-Straße 30, 22527 Hamburg
Telefon: +49 40 42883 2358
E-Mail: federrath@informatik.uni-hamburg.de

Nr.	Kürzel	Organisation	Ansprechpartner	Straße	PLZ, Ort	Telefon	E-Mail
1	UHH	Universität Hamburg, Arbeitsbereich Sicherheit in verteilten Systemen	Prof. Dr. Hannes Federrath	Vogt-Kölln-Straße 30	22527 Hamburg	+49 40 42883 2358	federrath@informatik.uni-hamburg.de
2	UBA	Universität Bamberg, Lehrstuhl für Privatsphäre und Sicherheit in Informationssystemen	Prof. Dr. Dominik Herrmann	An der Weberei 5	96047 Bamberg	+49 951 863 2661	dominik.herrmann@uni-bamberg.de
3	ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Harald Zwingelberg	Holstenstr. 98	24103 Kiel	+49 431 988 1222	ULD6@datenschutzzentrum.de
4	VOG	vogella GmbH	Jennifer Nerlich	Haindaalwisch 17a	22395 Hamburg	+49 40 7880436	jennifer.nerlich@vogella.com
5	QAB	Qabel GmbH	Oliver Weidner	Goseriede 4	30159 Hannover	+49 511 310166 00	weidner@qabel.de

Inhaltsverzeichnis

Zusammenfassung

Das Projekt EMPRI-DEVOPS beschäftigt sich mit technischen und rechtlichen Aspekten des Mitarbeiterdatenschutzes für Beschäftigte, die im Bereich der Software-Entwicklung und des IT-Betriebs (Development and IT Operations, DevOps) tätig sind. Diese Mitarbeiter sind besonderen Risiken ausgesetzt, da bei ihrer Arbeit sensible (Meta-) Daten anfallen. Die daraus entstehenden Risiken wurden bislang in der Wissenschaft vernachlässigt.

Im Projekt werden daher erstens die in gängigen DevOps-Tools anfallenden Daten systematisch erhoben. Zweitens wird untersucht, welche sensiblen Informationen daraus abgeleitet werden können, um die entstehenden Beeinträchtigungen für die informationelle Selbstbestimmung abschätzen zu können. Drittens werden für ausgewählte Werkzeuge mittels geeigneter datenschutzfördernder Mechanismen Demonstratoren entwickelt und evaluiert. Die technischen Arbeiten werden viertens durch eine Aufarbeitung rechtlicher Aspekte aus Sicht der aktuellen Gesetzgebung begleitet.

Zur Strukturierung der geplanten Analysen werden die Phasen des Software-Lebenszyklus (von der Konzeption bis zum Betrieb), die beteiligten Mitarbeiter-Rollen (u. a. Projektleiter, Systemarchitekten, Entwickler, Administratoren) und die verwendeten Werkzeug-Arten (z. B. Entwicklung mit Eclipse, Versionskontrolle mit Git, Issue-Tracking mit Jira, Kommunikation mit Slack sowie Monitoring mit Icinga) herangezogen. Gerade im Managed-Hosting-Segment ist zu erwarten, dass es zukünftig Bedarf an datenschutzfreundlichen DevOps-Systemen geben wird.

Das Verbundprojekt greift bei der Anforderungserhebung und Evaluation auf die Expertise zweier KMUs zurück und wird von einem assoziierten Projektbeirat unterstützt. Dadurch wird sichergestellt, dass die geschaffenen Lösungen den Bedürfnissen von Unternehmen und Entwicklern entsprechen. Die KMUs beabsichtigen, die Projektergebnisse (Demonstratoren und Leitfäden) für ihre eigenen Entwicklungsarbeiten einzusetzen und darüber hinaus nach dem Projektende als Produkt zur Marktreife zu bringen.

1 Thema und Zielsetzung

Die übergeordneten Tätigkeitsfelder des Projekts EMPRI-DEVOPS sind die Bewertung der Bedrohung der Privatsphäre durch die Überwachung von Mitarbeitern im Bereich Development and IT Operations [5] und die Entwicklung und Evaluation von datenschutzfreundlichen Lösungen durch die Anwendung von Methoden aus dem Gebiet des technischen Datenschutzes.

1.1 Relevanz und Umfeld

Dass Unternehmen grundsätzlich an einer datengetriebenen Analyse ihrer Mitarbeiter interessiert sind, belegt unter anderem eine von Bitkom Research und LinkedIn in Auftrag gegebene Studie [8]. Demnach erwarteten im Jahr 2015 etwa drei Viertel der Personalverantwortlichen von Big-Data-Analysen bessere Entscheidungsgrundlagen vor allem für ihre Kernaufgaben wie die Mitarbeitergewinnung, die Personaleinsatzplanung und das Controlling.

Zur Überwachung bereits vorhandener Mitarbeiter werden nach [35] einige Konzepte aus der Quantified-Self-Bewegung adaptiert und unter dem Begriff *Quantified Workplace* auf die Arbeitswelt übertragen: Sensoren am Arbeitsplatz oder im Mitarbeiter-Ausweis sollen u. a. Sitzhaltung, Kommunikationsverhalten und Puls auswerten [31]. Bei der datengetriebenen Optimierung der Mitarbeitergewinnung wird hingegen beispielsweise ein automatischer Abgleich der Facebook-Profile und Lebensläufe von Bewerbern vorgenommen [58]. Dies wird dann als *People Analytics* bezeichnet. Der Einsatz von solchen Analysen beeinträchtigt die informationelle Selbstbestimmung von Mitarbeitern und Bewerbern, insbesondere dann, wenn diese nicht nachvollziehen können, welche Daten über sie erhoben werden und welche Folgen dies für sie hat (Risiko der Diskriminierung).

1.2 Spezifika der Problemstellung

Mitarbeiter, die im DevOps-Bereich tätig sind, sind – neben den vorstehend genannten Überwachungsmöglichkeiten – einem besonderen Risiko der datengetriebenen Überwachung ausgesetzt. Ihre Aktivitäten lassen sich auch ohne physikalische Sensoren überwachen, weil sie bei vielen Tätigkeiten strukturierte (d. h. leicht auswertbare) Daten generieren, etwa in Form von Metadaten (z. B. Zeitpunkt, Ort und Art einer Aktivität). Dafür gibt es zwei Gründe:

1. Die Tool-Unterstützung ist im DevOps-Bereich weit fortgeschritten:
   - Änderungen am Quellcode werden in Versionskontrollsysteme eingecheckt.
   - Über den Prozess der Fehlerbehebung wird in Ticket-Systemen Buch geführt.
   - Die Kommunikation im Team findet in programmierbaren Messaging-Clients statt.
2. Es gibt eine ausgeprägte Bereitschaft zur Datenerfassung und -auswertung:
   - Agile Methoden optimieren die Produktivität von Teams anhand von Kennzahlen.
   - Performanz und Sicherheit der betriebenen Systeme werden kontinuierlich überwacht.

Diese Datenerhebung ist nicht nur für Arbeitgeber und Projektmanager nützlich, sie wird paradoxerweise auch von den Mitarbeitern geschätzt. Erst durch die daraus resultierende Nachvollziehbarkeit lassen sich komplexe Software-Projekte effektiv und mit ingenieurmäßiger Gründlichkeit durchführen. Integrierte Kommunikationslösungen erhöhen zudem die Effizienz, und für den zuverlässigen und sicheren Betrieb einer IT-Lösung ist eine kontinuierliche Kontrolle unerlässlich.

Dennoch steht diese Datenerhebung im Widerspruch zum Beschäftigtendatenschutz. Grundsätzlich könnten Arbeitgeber (oder Projektmanager und Controller) die erhobenen Daten nutzen, um die Leistungsfähigkeit von Mitarbeitern verdeckt zu beurteilen. Wegen der zunehmend populärer werdenden mobilen Arbeit oder Arbeit im Home-Office könnte ein Arbeitgeber mitunter auch Informationen über die privaten Lebensumstände und Aufenthaltsorte seiner Mitarbeiter gewinnen, etwa wenn IP-Adressen Rückschlüsse auf den Aufenthaltsort zulassen.

Detaillierte Zeitprotokolle lassen auf die Lebens- und Arbeitsgewohnheiten der Beschäftigten schließen, die Informationen preisgeben jenseits der bloßen Feststellung, ob die erforderliche Arbeitszeit im vereinbarten Zeitkorridor erbracht wurde. Generell erwachsen daraus Möglichkeiten zur missbräuchlichen Überwachung von Mitarbeitern.

Übermäßige Überwachung birgt allerdings auch Risiken für Arbeitgeber. Bei unzulässiger Datenverarbeitung drohen Geldbußen, arbeitsgerichtliche Verfahren und Image-Verlust. Tätigkeiten im Außendienst und Heimarbeit verlieren dadurch für einen Teil der Beschäftigten ihre besondere Attraktivität.

Eine heimliche Überwachung von Mitarbeitern ist im Regelfall unzulässig, wie das Bundesarbeitsgericht jüngst entschieden hat (Urteil vom 27. Juli 2017, 2 AZR 681/16). Anders als bei bisherigen People-Analytics-Ansätzen fällt es den Betroffenen im DevOps-Bereich allerdings ungleich schwerer, den Schutz ihrer Privatsphäre durchzusetzen. Die verdeckte Auswertung von Metadaten, die dort im normalen Betrieb ohnehin anfallen, ist für die Betroffenen weder erkennbar (im Unterschied zu einer Videokamera) noch nachträglich nachweisbar (im Unterschied zu einem heimlich installierten Keylogger).

1.3 Beispiel GitHub

Im Folgenden wird am Beispiel des Versionskontrollsystems Git illustriert, welche Risiken sich für die Privatsphäre aus der Analyse der in der Software-Entwicklung anfallenden Metadaten ergeben. Git speichert bei der Einbuchung von Änderungen (Commit) neben Benutzername und E-Mail-Adresse auch den aktuellen Zeitstempel. Commit-Zeitstempel lassen Rückschlüsse auf Arbeitszeiteinteilung, Fehlzeiten und Mitarbeiterbeziehungen zu. Die daraus resultierenden Auswertungsmöglichkeiten bedrohen die informationelle Selbstbestimmung von Software-Entwicklern über das für die Arbeitsplanung und Qualitätssicherung anzuerkennende Maß hinaus. Dass sich daraus sensible Informationen ableiten lassen, verdeutlicht das Beispiel der sogenannten Punch-Cards (s. Abb. 1), die den Zusammenhang zwischen Tageszeit und Commit-Aufkommen veranschaulichen. Der Anbieter GitHub etwa machte solche Punch-Cards (zumindest für öffentliche Repositories) frei im Internet zugänglich.

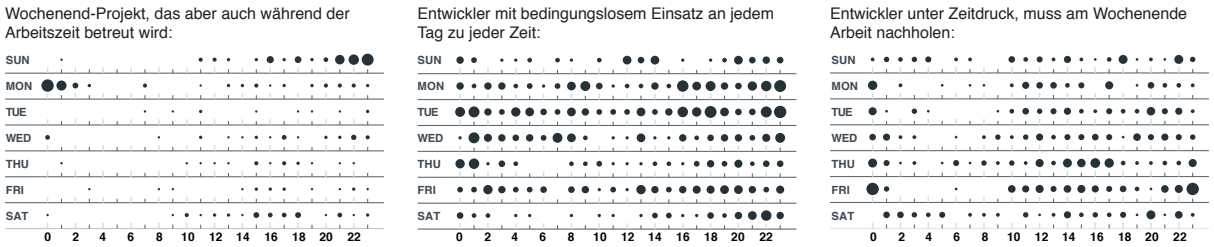

Abbildung 1: Punch-Cards von GitHub erlauben Einblicke in das Leben von Entwicklern [55]

1.4 Strukturierung des Projekts

Das Projekt EMPRI-DEVOPS beabsichtigt, die Problemstellung aus verschiedenen Perspektiven zu beleuchten, um alle wesentlichen Aspekte zu erfassen. Im Folgenden wird die geplante Strukturierung skizziert, mit der das erste Projektziel verfolgt wird, d. h. die systematische Erhebung der in DevOps-Werkzeugen anfallenden Daten. Das zweite Projektziel besteht darin, experimentell zu ermitteln, welche sensiblen Information sich aus den anfallenden Daten ableiten lassen (Inferenzrisiken). Die weiteren Projektziele der Implementation und Evaluation datenschutzfreundlicher Demonstratoren sowie die Aufarbeitung rechtlicher Fragestellungen werden anschließend dargestellt.

Wie in der Informationssicherheit üblich werden zunächst Angreifer sowie deren Fähigkeiten und Intentionen modelliert. Neben der Unternehmensleitung (A1) bzw. den von ihr mit der Überwachung von Mitarbeitern beauftragten Projektleitern (A2) oder Controllern (A3) kommen auch Kollegen (A4) als „Angreifer“ in Betracht.

In manchen Situationen können auch Außenstehende (A5) Mitarbeiter überwachen, etwa wenn ein Unternehmen Code auf im Internet (z. B. auf GitHub) veröffentlicht oder einen öffentlich einsehbaren Bug-Tracker bereitstellt. Als Angreifer kann auch die Personalabteilung (A6) eines Unternehmens definiert werden, die sich über die Persönlichkeit eines Bewerbers informiert, indem sie dessen im Internet veröffentlichte Open-Source-Repositories auswertet. Mit Blick auf die Rechtslage unterliegen insbesondere Datentransfers in Drittstaaten nach der DSGVO besonderen Anforderungen an die Datensicherheit und Transparenz. In der Betrachtung sind die identifizierten Angreifer daher auch nach deren geografischem bzw. rechtlichen Sitz zu beurteilen [13, S. 196], speziell zum Mitarbeiter-Screening auf Grund rechtlicher Anforderungen aus Drittstaaten [16].

Neben den Überwachungsabsichten werden auch die erwünschten Datenverwendungen sowie die Interessen der Mitarbeiter berücksichtigt. Dadurch lassen sich systematisch Zielkonflikte identifizieren, woraus sich Anforderungen an Mechanismen des technischen Datenschutzes formulieren lassen (sog. mehrseitige Sicherheit) [48], um die Sicherheitsinteressen und funktionalen Anforderungen aller Beteiligten angemessen zu berücksichtigen.

Eine weitere Perspektive auf die Problemstellung ist die Betrachtung der verschiedenen Phasen des Software-Lebenszyklus (s. Abb. 2). Diese Phasen sind dadurch gekennzeichnet, dass Mitarbeiter in verschiedenen Rollen daran beteiligt sind. Diese unterscheiden sich hinsichtlich ihrer Kenntnisse, Fähigkeiten und Berechtigungen. Es ist daher zu vermuten, dass verschiedene mentale Modelle bezüglich der ableitbaren Informationen und des Schutzes vor Überwachung vorherrschen. Diese sind bei der Entwicklung datenschutzfreundlicher Lösungen zu berücksichtigen. Ein Teilziel des Projekts EMPRI-DEVOPS besteht daher darin, zu ergründen, wie

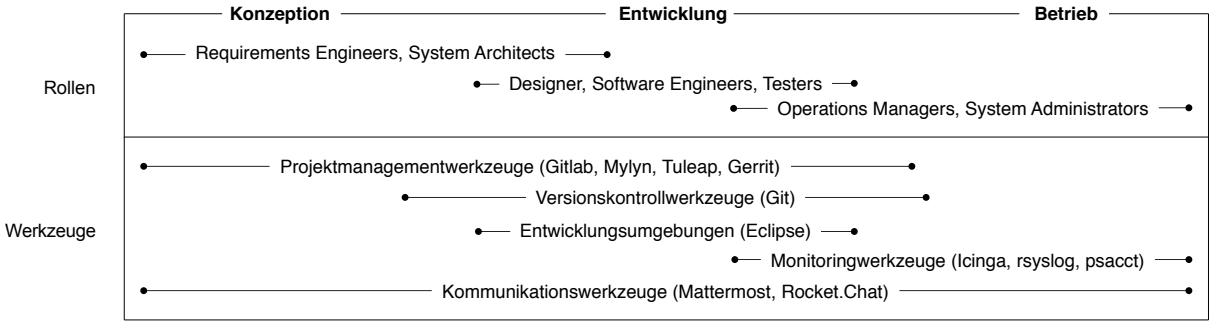

Abbildung 2: Ausgewählte Phasen des Software-Lebenszyklus mit relevanten Mitarbeiterrollen und Werkzeugen

Mitarbeiter in verschiedenen Rollen die Überwachungsmöglichkeiten und ihre Risikoexposition einschätzen bzw. wie sie die Notwendigkeit und Benutzbarkeit bestimmter Schutzmechanismen bewerten. Dazu werden in Arbeitspaket 1 eine Befragung und in Arbeitspaket 4 „Nutzer“-Tests mit Mitarbeitern in verschiedenen Rollen durchgeführt.

Daneben werden in den Phasen verschiedene Werkzeugtypen eingesetzt, die wiederum verschiedene Arten von (Meta-) Daten speichern. Abb. 2 nennt populäre Vertreter, deren Untersuchung im Hinblick auf mögliche Risiken durch Inferenzangriffe geplant ist (Arbeitspaket 2).

Das dritte Projektziel ist die Entwicklung von datenschutzfreundlich realisierten Demonstratoren. Dazu soll in Arbeitspaket 3 je ein Werkzeug aus den Kategorien Versionskontrolle, Issue-Tracking, Kommunikation und Monitoring entwickelt werden. Hierbei ist geplant, zwei unterschiedliche Lösungsansätze zu verfolgen, um die Zielkonflikte zwischen dem Schutz der Privatsphäre der Mitarbeiter und den erwünschten Möglichkeiten zur Auswertung von DevOps-Daten aufzulösen:

1. *Privacy Enhancing Technologies:* Durch Unterbinden oder Verrauschen werden bereits die Erfassung bzw. zumindest die Auswertung von potenziell sensiblen Daten vermieden. Dies geht allerdings u. U. mit einem Verlust der erwünschten Auswertungsmöglichkeiten einher.
2. *Transparency Enhancing Technologies:* Potenziell sensible Daten werden wie gehabt erfasst. Den Betroffenen werden technische Lösungen zur Verfügung gestellt, mit denen sie die Datenerfassung und die daraus ableitbaren Informationen einsehen und nachvollziehen und ggf. auf Wunsch unterbinden können. Wenn auf die Daten zugegriffen wird, dann stellen technische Mechanismen sicher, dass der Betroffene darüber benachrichtigt wird.

Auf der organisatorischen Ebene sind weiterhin verbindlich ergangene Vereinbarungen (z. B. Betriebsvereinbarungen bzw. Dienstvereinbarungen) erforderlich, um einen Einsatz der zuvor genannten Varianten zu ermöglichen. So ist beispielsweise in Schleswig-Holstein die Kontrolle der Internetnutzung der Landesbediensteten in einer Vereinbarung nach § 59 MBG-SH mit einer stufenweisen Eskalationsmöglichkeit bei Protokollauswertung und Sanktionierung versehen [22, Ziff. 6].

Die entwickelten Demonstratoren werden im Arbeitspaket 4 hinsichtlich ihrer Benutzbarkeit und Wirksamkeit evaluiert.

Das vierte Projektziel besteht in der Aufarbeitung rechtlicher Aspekte. Durch die Ablösung der nationalen Rechte durch die Europäische Datenschutz-Grundverordnung ist dieser Bereich in starkem Wandel. Die Teilmaterie des Beschäftigtendatenschutzes harrt dabei insbesondere weiterer nationaler Konkretisierungen. Die Artikel-29-Datenschutzgruppe hat insoweit mit dem Working Paper [3] bereits Akzente gesetzt. Die noch in starker Veränderung befindliche Rechtslage wird in EMPRI-DEVOPS aufgearbeitet, aktuelle Entwicklungen im Projekt gegenüber Dritten sowie Stakeholdern vermittelt und zur öffentlichen Diskussion über die Rechtsentwicklung beigetragen. In enger Verzahnung mit den anderen Arbeitspaketen werden Anforderungen für die Demonstratoren aufgestellt, für den Testbetrieb erforderliche Muster-Dokumente erstellt und eine abschließende Bewertung auf Basis der Methodik für Datenschutz-Folgenabschätzungen durchgeführt.

1.5 Bezug zu den förderpolitischen Zielen

Das Projekt EMPRI-DEVOPS adressiert mit seinen Projektzielen die folgenden Schwerpunkte aus der Bekanntmachung: Erstens die Schaffung praxistauglicher Realisierungsvarianten für den technikgestützten Beschäftigtendatenschutz, zweitens das Ausbalancieren von Zielkonflikten hinsichtlich Privatheit, Reputation und Nachweispflichten bei neuen Arbeitsformen und drittens Konzepte und Systeme zur Schaffung von Transparenz über betriebliche Datenverarbeitungsvorgänge.

2 Stand von Wissenschaft und Technik

2.1 Technische Sicht

Um die Projektziele anwendungsnah bearbeiten zu können, wurden für das Projekt konkrete DevOps-Werkzeuge ausgewählt (geplante Auswahl ist in Klammern angegeben). Dabei handelt es sich um populäre Open-Source-Werkzeuge. Die Popularität begünstigt die Reichweite und Anschlussfähigkeit der Ergebnisse, da aus dem großen Nutzerkreis mit höherer Wahrscheinlichkeit Interessenten für eine Fortführung gefunden werden. Für jede der betrachteten Werkzeug-Kategorien werden im Folgenden Risiken für die Privatsphäre dargestellt. Danach werden Ansätze zum Schutz der Privatsphäre und die Neuheit des Lösungsansatzes erläutert.

Versionskontrollsysteme (z.B. Git) In der Praxis konzentrieren sich die Arbeiten in diesem Bereich auf sensible Inhaltsdaten, etwa unabsichtlich veröffentlichte Passwörter und API-Keys [25]. In EMPRI-DEVOPS steht hingegen das Risiko der Analyse von Metadaten im Vordergrund, das in der Praxis bislang noch überhaupt nicht diskutiert wird. In der Wissenschaft wird bereits seit Jahren unter den Bezeichnungen „Mining Software Repositories“ und „Software Intelligence“ daran gearbeitet, aus Repository-Daten und -Metadaten auf Persönlichkeitsmerkmale [57], soziales Netz [50], Expertise [63], Belastungsgrad [11] und Produktivität eines Entwicklers zu schließen [34, 47, 51]. Arbeitgeber können sich diese Erkenntnisse bei der Personalgewinnung zunutze machen [64]. Für Inhouse-Auswertungen von Git-Repositories gibt es bereits kommerzielle Business-Intelligence-Lösungen [19]. Obwohl Entwickler Auswertungen ablehnen, anhand derer sich auf ihre Produktivität schließen lässt [6], wird ihre Privatsphäre bislang meist überhaupt nicht oder nur unzureichend geschützt. So bietet

das deterministische Pseudonymisieren von Identifikatoren mittels einer Hashfunktion keinen zuverlässigen Schutz [59, 44].

In EMPRI-DEVOPS werden daher Mechanismen des technischen Datenschutzes in das Versionskontrollsystem Git integriert, um unkontrollierte Profilbildung zu verhindern. Dabei betrachten wir mehrere zueinander komplementäre Ansätze, die sich an den generischen *Privacy Design Strategies* [12] orientieren. Ein erster Ansatz besteht dabei darin, die bei einem Commit anfallenden Metadaten zu verschleiern, etwa indem anstatt der tatsächlichen Uhrzeit lediglich eine gerasterte Zeitangabe gespeichert wird (z. B. auf ein Vielfaches von drei Stunden gerundet). Neben einer irreversiblen Verschleierung beim Abspeichern eines Commits kann dazu das Git-Backend auch so modifiziert werden, dass lediglich die Anzeige gerundet wird. Im Bedarfsfall könnten die genauen Zeitpunkte – die mit einem hybriden Kryptosystem verschlüsselt gespeichert wären – dann noch rekonstruiert werden.

Eine alternative oder komplementäre Strategie ist die Gewährleistung von Senderanonymität, also das Verbergen oder kontrollierte Anzeigen des Urhebers eines Commits (Name des Entwicklers, IP-Adresse seines Rechners), etwa durch die Verwendung von Transaktionspseudonymen und Mix-Netzen. Darüber hinaus sind noch tiefere Eingriffe vorstellbar, etwa aufeinanderfolgende Commits zusammenzufassen oder große Commits in mehrere kleine aufzuteilen. Schließlich werden auch kryptografische Schutzmechanismen betrachtet. So bietet sich die Verschlüsselung sensibler Informationen mit Schwellwert-Kryptosystemen an, mit denen ein Vier-Augen-Prinzip bei der Einsichtnahme durchgesetzt werden kann. So lässt sich die unkontrollierte Auswertung verhindern. Inwiefern dies zuverlässig, praxistauglich und gut benutzbar realisierbar ist, wurde bisher noch nicht untersucht.

Projektmanagementwerkzeuge (z.B. Gitlab, Mylyn, Tuleap, Gerrit) Auch im Bereich der Projektmanagementwerkzeuge (Issue-Tracker wie etwa in Gitlab, Anforderungsmanagement etwa mit Mylyn [20], agiles Projektmanagement etwa mit Tuleap [61], Code-Review-Prozesse mit Gerrit [23]), spielt der Schutz der Privatsphäre weder in Wissenschaft noch Praxis bislang eine Rolle. Einige Unternehmen betreiben ihre Projektmanagementwerkzeuge (v. a. Issue-Tracker) öffentlich und werben mit der daraus resultierenden Transparenz. Auch in geschlossenen Benutzergruppen gibt es jedoch Inferenzrisiken, welche die Privatsphäre der Entwickler bedrohen. Es ist schon länger bekannt, dass sich die Metadaten von Issue-Trackern dazu nutzen lassen, um die Effizienz und Effektivität von Entwicklern zu beurteilen [56]. Dies wird von kommerziellen Tools bereits unterstützt [26]. Zudem wurde 2016 festgestellt [42], dass sich durch Analyse der in Issue-Trackern hinterlegten Texte automatisiert auf den Gemütszustand von Entwicklern und auf Indikatoren für Burnout-Syndrome schließen lässt – ohne dabei auf die Implikationen für die Privatsphäre einzugehen.

Es ist daher zunächst zu untersuchen, inwiefern die Ergebnisse für Issue-Tracker auch auf andere Werkzeugarten in dieser Kategorie (Mylyn, Tuleap und Gerrit) übertragbar sind. Zum Schutz vor einer unerwünschten Auswertung eignen sich grundsätzlich dieselben Ansätze wie bei der Versionskontrolle (Verschleierung von Zeitstempeln, Senderanonymität und Schwellwert-Kryptosysteme). Als komplementäre Datenschutztechnik werden neben der vollständigen Verhinderung der Datenerfassung (die dementsprechend auch nützliche Auswertungen verhindert) zunehmend auch *Transparency-Enhancing-Technologies* einbezogen. In EMPRI-DEVOPS soll dazu ein *Privacy Dashboard* für Entwickler entworfen werden, das den Zugriff auf sensible Daten durch auditierbare Transparenz-Protokolldateien (etwa wie in [53] beschrieben) für

Entwickler nachvollziehbar macht. Privacy Dashboards und Transparenz-Logs wurden bislang lediglich im Konsumentenbereich untersucht [1].

Kommunikationswerkzeuge (z.B. Mattermost und Rocket.Chat) Entwickler kommunizieren heute mit zentralisierten Messaging-Systemen. Der Schutz der Privatsphäre ist bei solchen Systemen ein Thema, das in der Praxis lediglich im Hinblick auf Inhaltsdaten diskutiert wurde: Nutzer des populären kommerziellen Anbieters Slack waren sehr überrascht, dass sog. „private Chats“ von ihrem Arbeitgeber mitgelesen werden können [9]. Dies trifft auch auf das Open-Source-System Mattermost zu, bei dem Nutzer und Entwickler seit einiger Zeit über die Verschlüsselung privater Chats diskutieren [46], bislang allerdings ohne erkennbaren Fortschritt [45]. In dieser Debatte wird zudem übersehen, dass es besser geeignete Verfahren gibt [62] und dass das Verschlüsseln der Chats nicht die Verkehrsdaten verbirgt, also wer wann mit wem und wie oft interagiert. Mit angepassten Mix-Netzen oder speziellen Onion-Routing-Verfahren wie [39] lässt sich *Beziehungsanonymität* herstellen. Geeignete Techniken sollen in EMPRI-DEVOPS in Mattermost und/oder Rocket.Chat integriert werden.

Integrierte Entwicklungsumgebungen (z.B. Eclipse) Im Gegensatz zu den bisher genannten Werkzeugen erscheinen integrierte Entwicklungsumgebungen (Integrated Development Environments, IDEs) zunächst im Hinblick auf den Schutz der Privatsphäre weniger kritisch, da sie keine (Meta-) Daten an eine zentrale Stelle übermitteln. Da Entwickler einen Großteil ihrer Zeit in einer IDE verbringen, lässt sich dort ihre Effektivität und Effizienz jedoch besonders gut messen [2]. Zudem existieren insbesondere in Eclipse ausgereifte Mechanismen, um sämtliche Aktivitäten in der IDE zu protokollieren. Inwiefern Arbeitgeber ihre Mitarbeiter dadurch tatsächlich überwachen können, ist zu untersuchen. Sie könnten daran interessiert sein, aus dem Benutzerverhalten auf die Sorgfalt eines Entwicklers zu schließen, etwa indem sie Tippfehler, Compilerfehler, Copy&Paste-Verhalten und Häufigkeit des Aufrufens der Dokumentation erfasst werden. Ferner sind einschlägige Ergebnisse aus dem Usability-Bereich [49] hinsichtlich ihrer Implikationen für die Privatsphäre zu untersuchen und es ist zu klären, inwiefern Teilnehmer, die im Rahmen von Eclipse-Usability-Studien in die Aufzeichnung einwilligen, dadurch unabsichtlich sensible Informationen über sich preisgeben. Als Schutzmechanismen kommen hier Techniken zur anonymisierten, jedoch authentifizierten Übermittlung von Daten in Betracht, etwa das System Anonize [32].

System-Monitoringwerkzeuge (z.B. Icinga, rsyslog, psacct) Diese Kategorie umfasst Werkzeuge zur Überwachung von Betriebsparametern (z. B. CPU-Last und Antwortzeit mit Icinga [33]) und Event- bzw. Log-Dateien (etwa mit rsyslog unter Linux). Ferner zählen dazu auch Accountingwerkzeuge wie psacct, mit denen die ausgeführten Prozesse und gestarteten Programme protokolliert werden können. Auch Systeme aus dem Bereich Security Incident & Event Management (SIEM) lassen sich hier verorten; diese werden jedoch vom Partner UHH bereits im BMBF-geförderten Verbundprojekt DREI („Datenschutz-respektierende Erkennung von Innentätern“) hinsichtlich des Schutzes der Privatsphäre untersucht. In EMPRI-DEVOPS soll zum einen untersucht werden, inwiefern Arbeitgeber oder neugierige Kollegen (die z. B. ihren Vorgesetzten überwachen möchten) aus scheinbar harmlosen Log-Einträgen und aufgezeichneten Betriebsparametern auf sensible Informationen (Anwesenheit, Aufenthaltsort, Nutzungsdauer) schließen können. Hierzu sind uns keine Forschungsarbeiten und keine in der Praxis eingesetzten Schutzmechanismen bekannt. Im Bereich der Anonymisierung von

Log-Dateien [24] und deren datenschutzfreundlichem Austausch mit anderen Unternehmen (*Security Alert Correlation* [40]) gibt es hingegen bereits wissenschaftliche Arbeiten, auf deren Basis in EMPRI-DEVOPS datenschutzfreundliche Systeme gestaltet werden sollen. Eine Neuerung im Vergleich zu den bisherigen Ansätzen wird dabei die Anwendung von *Revocable-Privacy-Techniken* [41] sein, mit denen sich die Anonymisierung unter bestimmten Umständen rückgängig machen lässt.

2.2 Rechtlich-organisatorische Sicht

Im Bereich der Rechtswissenschaften und des Datenschutzes bestätigten sich die im Bereich der Technik festgestellten Recherche-Ergebnisse. Eine Literaturrecherche nach Datenschutz und Softwareentwicklung ergibt primär Ergebnisse für Datenschutzaspekte, die als Anforderungen an die Software als Produkt und den Prozess der Planung und Gestaltung dieser Softwareaspekte relevant sind (für die Befassung im aufsichtsbehördlichen Bereich etwa [3, S. 12 ff.]). So befasst sich unter anderem das von den Projektpartnern UHH und ULD mit Förderung des BMBF im Bereich Selbstdatenschutz durchgeführte Projekt AppPETs mit der Gestaltung datenschutzfreundlicher Softwarebibliotheken für die Entwicklung von Apps. Aus dem Kreise der Datenschutzaufsichtsbehörden liegen Orientierungshilfen für die Gestaltung von Apps in Smartphone-Umgebungen vor [17], die sich entsprechend auch auf andere Softwareprodukte übertragen lassen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrem Beschluss vom 27. März 2014 [37, S. 2] Problembereiche identifiziert, die zur politischen Forderung eines gesonderten Arbeitnehmerdatenschutzgesetzes geführt haben, etwa

- die Erhebung und Verarbeitung von Bewerberdaten beispielsweise aus sozialen Netzwerken,
- die zunehmende Verschmelzung von Arbeit und Privatem,
- der Zwang zur beruflichen Nutzung von privaten Arbeitsmitteln wie Smartphones und Laptops und
- Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen.

Diese Aspekte treffen Beschäftigte im DevOps-Umfeld durch die besonders engmaschige, digitale Erfassung der Tätigkeit in gesteigertem Maß.

Die Nutzung privater Smartphones und Laptops bzw. das Gestatten privater Nutzung unternehmenseigener Geräte ist nicht nur bei Start-ups im IT-Bereich weit verbreitet. Die Geräte können teilweise Tastenanschläge so genau protokollieren, dass aus den entstehenden biometrischen Mustern weitergehende Rückschlüsse auf die Person möglich sind [52].

Kern des Projektes stellt indessen der Schutz von Mitarbeitern im Bereich der Softwareentwicklung dar. Der Beschäftigtendatenschutz ist in der Datenschutz-Community im Allgemeinen und bei den Aufsichtsbehörden ein bereits bekannter Themenkomplex. Die Forderung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder nach spezifischen gesetzlichen Regelungen im Bereich des Beschäftigtendatenschutzes besteht schon lange und wurde zuletzt 2014 gegenüber dem Bundestag bekräftigt [37]. Auf europäischer Ebene ist eine detaillierte Vereinheitlichung des Beschäftigtendatenschutzes im Rahmen der DSGVO nicht erfolgt, insbesondere konnten sich die im Entwurf des Europäischen Parlaments vorgesehenen

Präzisierungen nicht durchsetzen (Maschmann in [38, Art. 88 Rn. 4]). Art. 88 DSGVO sieht nunmehr eine Öffnungsklausel für eine nationale Gesetzgebung vor. Insoweit ist in Deutschland mit § 26 BDSG-neu eine solche Regelung für Arbeitnehmer erfolgt, welche die bisher bestehende spezialgesetzliche Regelung des § 32 BDSG a. F. fortsetzt [15, S. 96 f.]. Im Verhältnis zwischen DSGVO und BDSG-neu genießt die DSGVO Anwendungsvorrang, soweit nationale Regelungen im Widerspruch mit der DSGVO stehen (Selk in [21, Art. 88 Rn. 8]). Damit ist bei allen Schritten der Betrachtung auch das EU-Recht mit zu berücksichtigen und sorgfältig zu prüfen, ob § 26 BDSG-neu verordnungskonform auszulegen ist (zur Pflicht einer autonomen Auslegung auch der Öffnungsklausel Maschmann in [38, Art. 88 Rn. 8]). Die Artikel-29-Datenschutzgruppe hat mit dem Working Paper 249 [3] bereits eine Übersicht der zu berücksichtigenden allgemein in der Union anerkannten Grundsätze erstellt.

Schließlich ist im Rahmen der Projektlaufzeit mit weiteren Änderungen der Rechtslage zu rechnen. Insoweit bleibt es bei dem lange festgestellten Konkretisierungsbedarf, den auch der Bundesrat noch einmal ausdrücklich mit der Bitte an die Bundesregierung, einen entsprechenden Entwurf vorzulegen, bekräftigt hat [14, S. 32]. Gegenwärtig sind Unternehmen und öffentliche Stellen im Zugzwang, sich mit den geänderten Regelungen der DSGVO zu befassen, ein effektives Datenschutzmanagement aufzubauen sowie bestehende Strukturen an die neue Rechtslage anzupassen. Diese Ausgangssituation bietet für Forschungsprojekte einen interessanten Handlungsrahmen, der für entwickelte Lösungen einen Bedarf und langfristigen Einsatz verspricht. EMPRI-DEVOPS nutzt diese Gelegenheit, um einen schonenden Ausgleich der Interessen der Arbeitgeber und der Persönlichkeitsrechte der Beschäftigten durch geeignete Privacy und Transparency Enhancing Technologies sowie durch organisatorische Mechanismen zu gestalten. Ein solcher Interessensausgleich ist vom Gesetzgeber ausdrücklich im Rahmen der Gesetzesanwendung vorgesehen [15, S. 97] und auch bei kollektivrechtlicher Regelung nach Art. 88 (2) DSGVO zwingend.

In dieser Situation bleibt die datenschutzrechtliche Tätigkeit im Projekt nicht auf eine bloße Begleitung und Bewertung der technischen Entwicklung beschränkt. Eine solche Begleitung ist erforderlich, um z. B. Muster für Betriebs- und Dienstvereinbarungen zu entwerfen. Darüber hinaus können jedoch eigenständig organisatorische Maßnahmen entworfen werden, wo technische Maßnahmen nicht möglich sind oder z. B. um Teilaspekten der durch internationalen Datenverkehr von Beschäftigtendaten auftretenden Besonderheiten Rechnung zu tragen.

3 Notwendigkeit der Zuwendung

3.1 Wirtschaftliche Risiken

Für die am Projekt beteiligten KMUs sind der Aufwand und die Kosten zu hoch, um datenschutzfreundliche DevOps-Werkzeuge eigenständig zu entwickeln. Die beteiligten KMUs können zwar auf Vorarbeiten in der Entwicklung von DevOps-Werkzeugen (VOG) bzw. datenschutzfreundlichen Techniken (QAB) zurückgreifen, keines der beiden Unternehmen hat allerdings die Ressourcen, sich in beiden Gebieten Kompetenzen anzueignen. Erst durch die Förderung des Projekts werden die dafür notwendigen Kapazitäten geschaffen.

Die Forschungspartner, die sich am Projekt beteiligen und ihr Wissen bezüglich datenschutzfreundlicher Techniken zur Verfügung stellen, haben auf der anderen Seite derzeit nicht genügend Ressourcen, um Werkzeuge für alle DevOps-Anwendungsfälle zu verbessern. Zudem

fehlt ihnen der Zugang zu den Benutzern solcher Werkzeuge, die über das nötige Wissen zu aktuellen Trends sowie das Know-How, um benutzerfreundliche und zugleich ansprechende, marktwirksame Lösungen umzusetzen, verfügen.

Auch auf Seiten des Partners ULD sind Ressourcen zu einer derart eingehenden und vertieften Befassung mit einem Thema und Unterstützung der Entwicklung von datenschutzfördernden Technologien nicht vorhanden. Insbesondere sind die aus Landesmitteln bereitgestellten Ressourcen mit der Umsetzung der DSGVO bei öffentlichen und privaten Stellen im Land gebunden. Indes wird der geschaffene Mehrwert für die Datenschutz-Community und die eine solche datenschutzfreundliche Lösung einsetzenden Unternehmen als hoch betrachtet.

Auf EU-Ebene sind uns derzeit keine geeigneten Ausschreibungen bekannt.

3.2 Wissenschaftlich-technische Projektrisiken

Im Projektverlauf können die folgenden wissenschaftlich-technische Risiken auftreten. Bei der Analyse der Inferenzrisiken (AP 2) könnte ein Fund signifikanter Inferenzpotenziale ausbleiben. In AP 3 besteht das Risiko, dass für Inferenzgegenmaßnahmen keine oder keine praktikablen Privacy Enhancing Technologies identifiziert oder implementiert werden können. In diesen Fällen kann durch eine Schwerpunktverlagerung auf transparenzsteigernde Maßnahmen reagiert werden. Auch dadurch lässt sich eine Stärkung der Betroffenenrechte der Beschäftigten erzielen und nachgehend in AP 4 evaluieren. Bezüglich der Evaluation (AP 4) besteht das Risiko, nicht ausreichend Entwickler und Systemadministratoren als Tester gewinnen zu können. Ersatzweise kann hier auf Probanden aus dem universitären Umfeld zurückgegriffen werden.

Wie bereits dargestellt, ist eine weitere Änderung des Rechts absehbar, woraus ein Risiko für AP 5 resultiert. Diesem Risiko wird durch ein kontinuierliches Monitoring der Entwicklungen seitens des ULD und frühzeitige Unterrichtung der Projektteilnehmer begegnet. Da das ULD im Rahmen der vorhandenen Kernausstattung nicht sämtliche denkbaren Quellen bereitstellen kann, insbesondere zur ggf. notwendigen rechtsvergleichenden Betrachtung nicht die nötigen Quellen aus anderen Mitgliedstaaten vorhält, ist im Projektbudget ein entsprechender Posten für derartige Beschaffungen vorgesehen.

Insgesamt ist festzustellen, dass die wissenschaftlich-technischen Risiken während der Laufzeit des Vorhabens bewältigt werden können und somit den Projektfortgang nicht gefährden.

4 Marktpotenzial

Das Marktpotenzial für datenschutzfreundliche DevOps-Werkzeuge ist zum jetzigen Zeitpunkt kaum abschätzbar. Grundsätzlich herrscht jedoch ein positives Marktumfeld für EMPRI-DEVOPS, da wegen der datenschutzfreundlichen Gesetzgebung auf europäischer Ebene von einer ansteigenden Nachfrage auszugehen ist. Um eine hohe Akzeptanz der Lösungen zu erreichen, sollen die Demonstratoren und langfristig auch die daraus entstehenden Produkte als Open-Source-Software veröffentlicht werden. Das ändert jedoch nichts an der positiven Konkurrenzsituation für das Projekt, sowohl aus wissenschaftlicher als auch in wirtschaftlicher Hinsicht. Die Forschungspartner erhalten durch die Wirtschaftspartner Zugang zu Entwicklern, der für die Gestaltung gut benutzbarer Lösungen essenziell ist. Die Projektpartner und

die assoziierten Unternehmen erhalten durch die Beteiligung im Projekt einen Wissensvorsprung und können dadurch den Markt für datenschutzfreundliche DevOps-Werkzeuge schnell erschließen.

Die folgenden Betrachtungen vermitteln einen Eindruck von der Popularität von DevOps-Werkzeugen und belegen die Zahlungsbereitschaft im kommerziellen Umfeld. Versionskontrollwerkzeuge sind weit verbreitet: Der populäre Open-Source-Anbieter Gitlab verzeichnete im Januar 2016 mehr als 1,9 Mio. kumulative Downloads der Community Edition, die Unternehmen im eigenen Haus betreiben können [4]. Gitlab bietet Unternehmen auch das Outsourcing des Repositories an (Preisspanne zwischen 3 und 17 USD pro Nutzer und Monat). Gitlab-Hosting in Deutschland mit umfangreicheren Service-Leistungen wird vom assoziierten Partner NET für 50 bis 150 EUR pro Monat angeboten. Ein populärer Stellvertreter im Bereich der Kommunikationswerkzeuge ist Mattermost Classic, dessen Android-App mehr als 50 000 mal im Google Play-Store heruntergeladen worden ist. Die kommerzielle Variante Slack (über 5 000 000 Downloads) wird Unternehmenskunden zu Preisen zwischen 6 und 12 USD pro Nutzer und Monat angeboten. Die Alternative Rocket.Chat [60] wird von NET zu Preisen zwischen 25 und 100 EUR pro Monat angeboten. Der System-Monitoring-Markt soll bis 2025 ausgehend von einem Volumen von 19 Mrd. USD in 2015 bis 2024 jährlich um 6 % wachsen [54], der Teilbereich Log Management ausgehend von einem Marktvolumen von 700 Mio. USD bis 2022 jährlich um 12 % [43]. Icinga2-Hosting wird von NET für Preise zwischen 10 und 100 EUR pro Monat angeboten.

Dementsprechend ist von einem hohen Marktpotenzial für die Ergebnisse von EMPRI-DEVOPS auszugehen. Soweit das Projekt EMPRI-DEVOPS allgemeine Lösungsmodelle für den Arbeitnehmerdatenschutz im IT-Bereich entwickelt, können diese zudem gut auf andere und allgemeinere Bereiche der Arbeitswelt übertragen werden.

5 Kurzdarstellung der beantragenden Partner

Tabelle 1 zeigt die Hauptaufgaben der Projektpartner im Überblick. Ein Großteil der Partner kooperierte bereits mehrfach in anderen Forschungsprojekten.

5.1 Universität Hamburg (UHH)

Der Arbeitsbereich Sicherheit in verteilten Systemen (Prof. Dr. Hannes Federrath) ist dem Fachbereich Informatik der Universität Hamburg (UHH) zugeordnet. Die am Lehrstuhl vorhandene Kompetenz im Bereich Informationssicherheit deckt sowohl übergreifende Aspekte (Sicherheitsmanagement, mehrseitige Sicherheit, wirtschaftliche Aspekte) als auch Techniken der IT-Sicherheit (Authentifizierung, Autorisierung, Zugangskontrolle, digitale Signaturen, Public-Key-Infrastrukturen) ab. Einen Schwerpunkt bildet die Gestaltung und Evaluation von datenschutzfreundlichen Techniken zum Schutz der Privatsphäre. Als Vorarbeiten dienen Aktivitäten aus dem Bereich der Kommunikationsanonymität (u. a. im BMBF-Projekt AN.ON-next: „Anonymität Online der nächsten Generation“) und der Implementierung von kryptografischen Schwellwert-Schemata (u. a. im BMBF-Projekt DREI: „Datenschutzrespektierende Erkennung von Innentätern“). Zu den Aufgaben im Projekt EMPRI-DEVOPS zählen daher neben der Projektkoordination insbesondere Forschungsaktivitäten zur Analyse von Inferenzrisiken (AP 2)

UHH	Koordination Gesamtprojekt, AP 1 (Ist-Analyse) und AP 4 (Evaluation). Forschung zu Inferenzrisiken (AP 2) und zu benutzbaren Privacy bzw. Transparency Enhancing Technologies (Fokus: Versionskontrolle, AP 3).
UBA	Koordination AP 2 (Inferenzrisiken). Forschung zu Inferenzrisiken und der datenschutzfreundlichen Umsetzung von Projektmanagement- und Monitoring-Werkzeugen (AP 3).
ULD	Koordination AP 5 (Datenschutzrecht); Studien und projektbegleitende Beratung zu datenschutzrechtlichen Anforderungen und rechtskonformer Umsetzung; Organisation eines Workshops mit Stakeholdern (AP 6).
VOG	Koordination AP 3 (Konzeption & Entwicklung); Unterstützung v. Ist-Analyse und Evaluation (AP 1 und 4); Eclipse-Verbesserung (AP 3); Workshop mit Entwicklern (AP 6). Ergebnisverwertung: Aufnahme in eigene Angebotspalette.
QAB	Unterstützung der Ist-Analyse und der Evaluation (AP 1 und AP 4); Hosting der Demonstratoren. Ergebnisverwertung: firmeninterne Verwendung.

Tabelle 1: Hauptaufgaben der Projektpartner

sowie die Entwicklung gut benutzbarer Mechanismen des technischen Datenschutzes und deren Integration in DevOps-Werkzeuge (AP 3).

5.2 Otto-Friedrich-Universität Bamberg (UBA)

Der Lehrstuhl für Privatsphäre und Sicherheit in Informationssystemen (PSI, Prof. Dr. Dominik Herrmann) gehört zur Fakultät für Wirtschaftsinformatik und Angewandte Informatik der Otto-Friedrich-Universität Bamberg (UBA). Die Fakultät zeichnet sich insbesondere durch anwendungsorientierte Forschung aus. UBA ist durch den Lehrstuhl PSI in der Forschungs-, Kooperations- und Gründungsplattform Zentrum Digitalisierung.Bayern (ZD.B) vertreten und verfügt somit über ein kompetentes Netzwerk aus Vertretern der Wirtschaft, Wissenschaft und Verbänden, das auf einen interdisziplinären Wissenstransfer ausgelegt ist. UBA ist ferner in das H2020-Projekt CANVAS („Constructing an Alliance for Value-driven Cybersecurity“, https://canvas-project.eu) eingebunden, in dem Fragen der Sicherheit und der Privatsphäre aus technischer, ethischer und rechtsphilosophischer Sicht betrachtet werden [10]. Für EMPRI-DEVOPS besonders relevant sind Vorarbeiten auf dem Gebiet des Trackings von Internetnutzern anhand von Metadaten sowie die datenschutzfreundliche Gestaltung von Informationssystemen [28, 30] (ausgezeichnet mit dem GI-Dissertationspreis 2014 [27]). Weiterhin existieren Vorarbeiten im Bereich der Inferenzangriffe [29, 36], die in Verbindung mit einer Arbeitsgruppe für Maschinelles Lernen an der TU Kaiserslautern entstanden sind. Im Projekt EMPRI-DEVOPS liegt der Fokus von UBA daher auf der Ist-Analyse (AP 1), der Untersuchung des Risikos durch Inferenzangriffe (AP 2) und der Konzeption und Entwicklung von datenschutzfreundlichen Techniken (AP 3).

5.3 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ist die Aufsichtsbehörde für Datenschutz des Landes Schleswig-Holstein und eine rechtsfähige Anstalt des

öffentlichen Rechts mit Sitz in Kiel (§ 32 LDSG S-H). Träger der Anstalt ist das Land Schleswig-Holstein. Im ULD sind 40 Mitarbeiter beschäftigt. Das ULD berät und beaufsichtigt Schleswig-Holsteins öffentliche und nicht-öffentliche Stellen in allen Fragen des Datenschutzes und den damit verbundenen Fragen der Datensicherheit. Das ULD steht für die Implementierung von Datenschutz und Datensicherheit über eine proaktive Gestaltung der Technik, Beratung der Betroffenen, Hersteller und Anwender, Unterstützung datenschutzfördernder Techniken und Dienstleistungen sowie einen prozessorientierten Datenschutz. Als rechtlich unabhängige Einrichtung führt das ULD seit Jahren wissenschaftliche Studien und projektbegleitende Beratung durch, um innovative Ideen und Konzepte im Hinblick auf ihre rechtlichen, technischen und gesellschaftlichen Rahmenbedingungen zu prüfen und datenschutzgerechte Technikgestaltungen und -anwendungen zu fördern. Auftraggeber sind nationale und internationale, öffentliche und private Einrichtungen.

5.4 Qabel GmbH (QAB)

Die 2014 in Hannover gegründete Qabel GmbH (QAB, 7 Mitarbeiter) ist ein Hersteller von cloudbasierten, kryptografischen Softwarelösungen, die es jedermann ermöglichen, jegliche digitale Kommunikation und damit einhergehende Daten effektiv zu verschlüsseln. Die eigens entwickelten Technologien und Produkte werden im B2C-Bereich eingesetzt bzw. in bestehende Lösungen von Kunden aus dem B2B(2C)-Bereich integriert und sind fast ausschließlich Open-Source. Im Rahmen der CeBIT 2016 wurde mit „Qabel Box Public Beta“ ein verschlüsselter Onlinespeicher für Endverbraucher (B2C) unter großem Medienecho vorgestellt.

Für die hauseigene Entwicklung setzt QAB diverse DevOps-Werkzeuge zur Unterstützung ihrer agilen Prozesse ein. Der aus IT-Sicherheitssicht gebotenen Transparenz verpflichtet, findet die Entwicklung weitestgehend öffentlich auf GitHub statt (Source Code, Issues, Code Review). Dem Transparenzgebot stehen allerdings Datenschutzinteressen der Entwickler entgegen, weshalb QAB um einen angemessenen Ausgleich bemüht ist und regelmäßig alternative Werkzeuge erprobt.

Peter Leppelt, Gründer und Geschäftsführer von QAB, ist Mitglied des Digitalrates Niedersachsens. QAB ist als Ausgründung der praemandatum GmbH weiterhin in engem Kontakt und profitiert von deren Erfahrung aus den BMBF-geförderten Projekten AppPETs und SmartPriv.

QABs Aufgaben im Projekt EMPRI-DEVOPS umfassen daher die systematische Erhebung des Status Quo der eingesetzten DevOps-Werkzeuge sowie die Abbildung des Interessenkonflikts zwischen dem Beschäftigtendatenschutz und dem Datenbedarf agiler Prozesse. Des Weiteren evaluiert QAB die im Projekt entwickelten Demonstratoren für datenschutzfreundlichere DevOps-Werkzeuge in Teststellungen hinsichtlich ihrer Nutzbarkeit und Integrierbarkeit. Dabei profitiert QAB von der Erfahrung im Einsatz verschiedenster DevOps-Werkzeuge und von seinen bereits sensibilisierten Entwicklern und Systemadministratoren.

5.5 vogella GmbH (VOG)

Die Angebotspalette der in Hamburg ansässigen vogella GmbH (VOG, 5 Mitarbeiter) umfasst Beratung, Schulungen und Entwicklungen im Bereich von Software-Entwicklung mit Schwerpunkten auf Git, Eclipse und Android.

VOG verfolgt zwei Ziele: Die Optimierung von Open-Source-Software für den Unternehmenseinsatz und die direkte Unterstützung von Kunden in Software-Projekten. VOG und seine Kunden verwenden meist Git als Versionskontrollsystem sowie Issue-Tracker wie Bugzilla, GitHub Issues und Jira. Die vogella-Website ist Anlaufpunkt für etwa eine Million Softwareentwickler im Monat und damit eine der führenden Webseiten in diesem Bereich.

Geschäftsführer Lars Vogel ist Projektleiter im Eclipse-Projekt, welches von vielen Kunden verwendet wird. Mitarbeiter von VOG sind an der Entwicklung von Komponenten der Eclipse IDE beteiligt, etwa dem Git-Tooling und weiteren datenschutzrelevanten Komponenten wie der Integration des Issue-Trackers Mylyn.

Erfahrung mit Forschungsprojekten ist bei VOG bereits vorhanden. Derzeit arbeitet Geschäftsführerin Jennifer Nerlich etwa im EU-Projekt *OpenReq* (8 Konsortialpartner aus 6 Ländern) an der optimalen Auswahl und Klassifikation von Software-Anforderungen.

VOG steuert im Projekt EMPRI-DEVOPS seine Expertise bei der Analyse, Konzeption und Umsetzung von Open-Source-Ansätzen über den gesamten Software-Lebenszyklus bei. Insbesondere wird VOG im Rahmen der Ist-Analyse (AP 1) die Tracing-Möglichkeiten in Eclipse, dem Review-System Gerrit, bei Issue-Trackern (z. B. Mylyn) und Anforderungsmanagement-Systemen analysieren und diese in Zusammenarbeit mit UHH und UBA verbessern (AP 3) und evaluieren (AP 4). VOG arbeitet innerhalb seines Kundenstamms täglich mit den o. g. Tools und kennt deren Stärken und Schwächen. Zudem organisiert VOG den zweiten Workshop des Projekts.

5.6 Projektbeirat

Es wird ein Projektbeirat eingerichtet, der die Projektpartner bei der Durchführung berät. Dieser setzt sich (zum Zeitpunkt der Einreichung dieser Vorhabensbeschreibung) aus drei nachfolgend kurz beschriebenen, assoziierten Partnern zusammen.

Die Gascade Gastransport GmbH (GAS) unterstützt das Projekt aus der Perspektive eines IT-Anwender-Unternehmens. GAS verfügt über Inhouse-Expertise im Bereich IT-Operations und System-Monitoring. Lara Berdelsmann, die derzeitige Informationssicherheitsbeauftragte von GAS, war dort zuvor als IT-Operations-Managerin tätig und engagiert sich bei der Entwicklung des verbreiteten Open-Source-Monitoring-Werkzeugs Icinga [33].

Die NETWAYS GmbH (NET) unterstützt seit mehr als 15 Jahren Unternehmen beim Management komplexer IT-Umgebungen auf der Basis von Open-Source-Software. Neben Entwicklungsleistungen und Support bietet NET auch das Hosting und Managed-Services von DevOps-Werkzeugen wie Gitlab, Icinga und Rocket.Chat an. NET ist an den Ergebnissen von EMPRI-DEVOPS interessiert, um langfristig sein Portfolio mit datenschutzfreundlichen Lösungen zu ergänzen.

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF) ist ein Verein mit etwa 700 Mitgliedern aus Wissenschaft und Praxis, die sich u. a. für die menschengerechte Gestaltung von Arbeitsprozessen und gegen den Einsatz der Informationstechnik zur Kontrolle und Überwachung einsetzen. FIfF unterstützt das Projekt bei der Verbreitung der Ergebnisse, etwa in der Zeitschrift FIfF-Kommunikation.

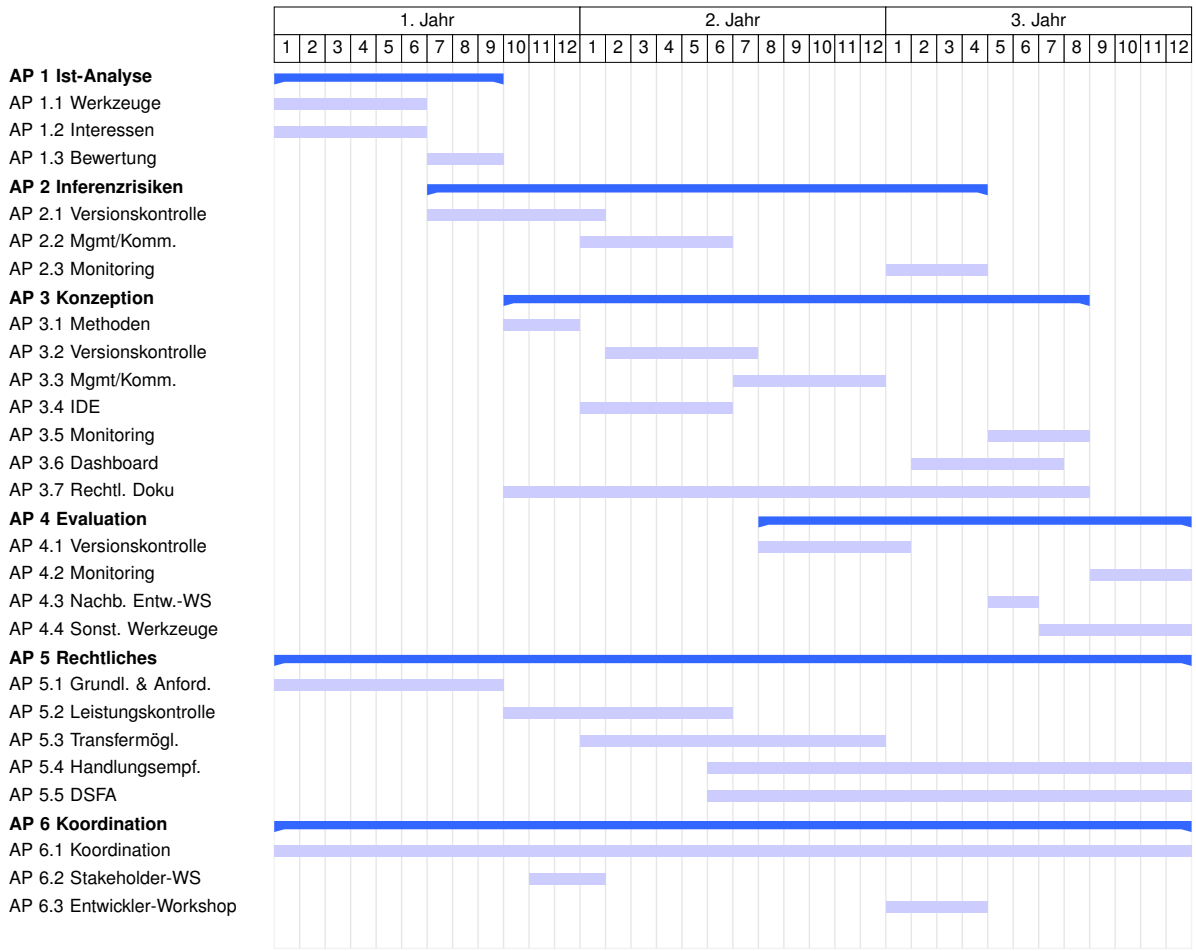

Abbildung 3: Zeitplan des Projekts

6 Arbeitsplan

Die für das Projekt erforderlichen Aktivitäten und wesentlichen Ergebnisse sind in sechs Arbeitspaketen (APs) strukturiert. Der zeitliche Ablauf ist in Abb. 3 veranschaulicht. Der geplante Start des Projekts ist November 2018. Für jedes Arbeitspaket sind im Folgenden die Ziele und jeweiligen Unterarbeitspakete (Zahlen in Klammern: Personenmonate pro Partner) mit ihren wesentlichen Meilensteinen/Ergebnissen (mit Fertigstellungsmonat) aufgeführt.

AP 1: Ist-Analyse

UHH 5 PM, UBA 9 PM, ULD 3 PM, VOG 9 PM, QAB 6 PM

In AP 1 wird der Status Quo der betrachteten DevOps-Werkzeuge und ihrer typischen Einsatzbedingungen untersucht. Zum einen findet eine Analyse des Erhebungs- und Protokollierungsverhaltens der Werkzeuge im Hinblick auf personenbezogene Daten der Beschäftigten statt, zum andern werden die verschiedenen Verarbeitungsinteressen von Arbeitgebern und verantwortlichen Mitarbeitern untersucht. Hierzu werden in enger Zusammenarbeit mit QAB und VOG die Einsatzsituationen in den Unternehmen erfasst und dokumentiert. Die Bestandsaufnahme der Interessen stellt dabei die Grundlage der weiteren Prüfung der Rechtsgrundlagen in AP 5 dar. Umgekehrt beeinflussen rechtlichen Anforderungen die Interessenlage der Sta-

keholder (handels- oder steuerrechtliche Dokumentationspflichten, Pflichten gegenüber den Auftraggebern).

Unterarbeitspakete

AP 1.1: Analyse der Werkzeuge (UHH 5, VOG 3, QAB 3)

AP 1.2: Analyse der Verarbeitungsinteressen (UBA 6, ULD 3, VOG 3, QAB 3)

AP 1.3: Bewertung der Analyse-Ergebnisse (UBA 3, VOG 3)

Meilensteine

E1 Bericht zu Werkzeugen und Interessen (M9)

AP 2: Inferenzrisiken

UBA 10 PM, UHH 5 PM, ULD 3 PM

AP 2 dient der Abschätzung der Risiken für die Informationelle Selbstbestimmung der Beschäftigten. Mittels gängiger Inferenz-Verfahren [57, 50, 63] werden repräsentativ gewonnene Datensätze aus DevOps-Werkzeugen (z. B. öffentliche Git-Repositories) dahingehend untersucht, welche nichttrivialen Aussagen über Leistung und Verhalten der betroffenen Beschäftigten ableitbar sind. Das so ermittelte Risikopotenzial ist die Basis für die Risikobewertung in einer Datenschutz-Folgenabschätzung (DSFA). Bereits in dieser Phase beteiligt sich das ULD, um eine spätere Verwendungsfähigkeit für die DSFA sicherzustellen und rechtliche Aspekte bei der Gewichtung der Risiken einfließen zu lassen.

Unterarbeitspakete

AP 2.1: Risikoanalyse von Versionskontrollwerkzeugen (UHH 5, ULD 1)

AP 2.2: Risikoanalyse von Management- und -kommunikationswerkzeugen (UBA 6, ULD 1)

AP 2.3: Risikoanalyse von Monitoring-Werkzeugen (z. B. Nagios) (UBA 4, ULD 1)

Meilensteine

E2.1 Bericht zu Inferenzrisiken in Versionskontrollwerkzeugen (M12)

E2.2 Bericht zu Inferenzrisiken in Management- und Kommunikationswerkzeugen (M18)

E2.3 Bericht zu Inferenzrisiken in Monitoringwerkzeugen (M28)

AP 3: Konzeption und Entwicklung

VOG 15 PM, UHH 12 PM, UBA 13 PM, ULD 4 PM, QAB 1 PM

In AP 3 werden für die untersuchten Werkzeuge Konzepte erstellt, wie die zuvor identifizierten Risiken durch den Einsatz von Privacy bzw. Transparency Enhancing Technologies (Reduktion von Metadaten, Differential Privacy [18]) zu einem angemessenen Ausgleich mit den Verarbeitungsinteressen des Arbeitgebers gebracht werden können. Für die jeweiligen Einsatzzwecke werden populäre Open-Source-Werkzeuge entsprechend datenschutzfördernd modifiziert.

Unterarbeitspakete

AP 3.1: Festlegung der Methodik zur Anpassung der Werkzeuge (UBA 3, VOG 3, QAB 1)

AP 3.2: Anpassung von Versionskontrollwerkzeugen (UHH 6)

AP 3.3: Anpassung von Management- und Kommunikationswerkzeugen (UBA 6, VOG 6)

AP 3.4: Anpassung Integrierter Entwicklungsumgebungen (VOG 6)

AP 3.5: Anpassung von Monitoring-Werkzeugen (UBA 4)

AP 3.6: Entwicklung eines Dashboards zur Transparenz-Gewährleistung (UHH 6)

AP 3.7: Datenschutzkonforme Dokumentation, Rechtsgrundlagen, Muster kollektivrechtl. Vereinbarungen (ULD 4)

Meilensteine

E3.1 Demonstrator Versionskontrolle (M18)

E3.2 Demonstrator Projektmanagement und -kommunikation (M24)

E3.3 Demonstrator IDE (M24)

E3.4 Demonstrator Monitoring (M32)

E3.5 Demonstrator Dashboard (M30)

AP 4: Evaluation **UHH 10 PM**, UBA 4 PM, QAB 10 PM, VOG 8 PM

AP 4 widmet sich der Evaluation und iterativen Verbesserung der in AP 3 entwickelten Demonstratoren. Die Evaluation umfasst zum einen einen Vorher-Nachher-Vergleich der in AP 2 ermittelten Inferenzrisiken mit den verbleibenden Möglichkeiten bei Nutzung der angepassten Demonstratoren aus AP 3. Zum anderen werden die Demonstratoren testweise den Mitarbeitern von QAB und VOG zur Verfügung gestellt. Diese evaluieren sowohl die Benutzbarkeit als auch die Integrierbarkeit in bestehende Arbeitsabläufe und Infrastrukturgegebenheiten. Dazu werden in den Unternehmen Nutzertests mit Projektmanagern, Systemarchitekten, Entwicklern und Systemadministratoren durchgeführt.

Unterarbeitspakete

AP 4.1: Evaluation der angepassten Versionskontrollwerkzeuge (UHH 5, QAB 4)

AP 4.2: Evaluation der angepassten Monitoringwerkzeuge (UBA 4)

AP 4.3: Nachbereitung des Entwicklerworkshops aus AP6.3 (VOG 2)

AP 4.4: Evaluation sonstiger angepasster Werkzeuge (UHH 5, VOG 6, QAB 6)

Meilensteine

E4.1 Workshop-Dokumentation (M30)

E4.2 Evaluationsbereicht (M36)

AP 5: Rechtliche Aspekte **ULD 23 PM**

AP 5 überdauert als Arbeitspaket die gesamte Projektlaufzeit und weist enge Verbindungen zu den anderen AP auf. Während die Kern-Expertise des ULD im Bereich des Datenschutzrechts liegt, werden, soweit für die Betrachtung erforderlich, auch Aspekte anderer Rechtsgebiete, insbesondere des Individual- und Kollektivarbeitsrechts, Rechtsmaterien im Zusammenhang mit Herstellung und Vertrieb von Software und mögliche Verpflichtungen der Arbeitgeber zur Datenverarbeitung betrachtet.

Hinsichtlich der Bestimmung des Rechtsrahmens ist eine Darstellung der Rechtsgrundlagen und Anforderungen des § 26 BDSG-neu und der DSGVO vorgesehen. Die Anforderungen werden nach dem Muster des von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder empfohlenen Standarddatenschutzmodells (SDM) gegliedert und für die weitere Verwendung in der Praxis aufbereitet. Die auf dem SDM basierende Methodik zur Datenschutz-Folgenabschätzung (DSFA) wird gegenwärtig von den Deutschen Aufsichtsbehörden gegenüber der Artikel-29-Datenschutzgruppe als Muster für eine DSFA auf europäischer Ebene vorgeschlagen und kontinuierlich fortentwickelt (vergl. [7]).

Unterarbeitspakete

AP 5.1: Datenschutzrechtliche Grundlagen und Anforderungen (ULD 4)

AP 5.2: Verhaltens- und Leistungskontrolle im Beschäftigungskontext (ULD 4)

AP 5.3: Transfermöglichkeiten für digitale Arbeitswelten (ULD 5)

AP 5.4: Handlungsempfehlungen (ULD 5)

AP 5.5: Datenschutz-Folgenabschätzung (ULD 5)

Meilensteine

E5.1 Gutachten zum Beschäftigtendatenschutz in der digitalen Arbeitswelt (M18)

E5.2 Gutachten DSFA, Ergebnistransfer, Muster-Dokumente (M36)

AP 6: Koordination und Ergebnisverbreitung **UHH 4 PM**, ULD 3 PM, VOG 4 PM, QAB 1 PM

AP 6 ist für die Projektkoordination vorgesehen. Neben der Anfertigung von Berichten und der Organisation von zwei Projekttreffen pro Jahr ist die Bereitstellung einer Arbeitsumgebung (Dokumentenvorlagen, Kalender, Versionskontrolle) sowie die Erstellung und der Betrieb einer öffentlichen Projektwebsite vorgesehen. Darüber hinaus ist die Organisation und Durchführung von zwei Workshops geplant. Diese dienen der Einbeziehung von und Diskussion der Zwischenergebnisse mit Stakeholdern aus Wirtschaftsverbänden (Bitkom und eco), Gewerkschaften (DGB und Verdi) und weiteren Interessenvertretern (GI, GDD und BvD) und der Verbreitung der Ergebnisse. In Tutorien soll die Verwendung der entwickelten Demonstratoren vermittelt werden.

Unterarbeitspakete

AP 6.1: Projektkoordination (UHH 4)

AP 6.2: Stakeholder-Workshop mit Vor- und Nachbereitung (ULD 3)

AP 6.3: Entwickler-Workshop (VOG 4, QAB 1)

Meilensteine

E6.1 Bericht zum Stakeholder-Workshop (M13)

E6.2 Demonstratoren und -bericht zum Entwickler-Workshop (M28)

7 Finanzierungsplan

(fehlt in dieser Version)

8 Verwertungsplan

(fehlt in dieser Version)

Literatur

[1] Julio Angulo u. a. „Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures“. In: *CHI*. ACM, 2015, S. 1803–1808.

[2] Gábor Antal u. a. „A methodology for measuring software development productivity using Eclipse IDE“. In: *ICAI*. 2014.

[3] Article 29 Data Protection Working Party. *Opinion 2/2017 on data processing at work. Adopted on 8 June 2017*. 2017.

[4] Luke Babb. *2015 was a great year at GitLab!* 2016. URL: https://about.gitlab.com/2016/02/11/gitlab-retrospective/.

[5] Len Bass u. a. *DevOps: A Software Architect's Perspective*. 1st. Addison-Wesley, 2015.

[6] Andrew Begel und Thomas Zimmermann. „Analyze this! 145 questions for data scientists in software engineering“. In: *ICSE*. ACM, 2014, S. 12–13.

[7] Felix Bieker u. a. „Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung“. In: *Recht der Datenverarbeitung (RDV)* 32 (2016), S. 188–197.

[8] bitkom research. *„Big Data“ verändert das Personalwesen nachhaltig*. URL: https://www.bitkom-research.de/Presse/Pressearchiv-2015/0518.

[9] Cynthia Boris. *Your private Slack conversations, might not be private at all*. URL: https://reputationrefinery.com/slack-privacy-issues.

[10] Markus Christen u. a. „Beyond informed consent – investigating ethical justifications for disclosing, donating or sharing personal data in research“. In: *Joint conference of the International Society for Ethics and Information Technology and the International Association for Computing and Philosophy*. s.n., Juni 2015.

[11] Maëlick Claes u. a. „Do Programmers Work at Night or During the Weekend?“ In: *Proceedings of the 40th International Conference on Software Engineering*. ICSE '18. Gothenburg, Sweden: ACM, 2018, S. 705–715.

[12] Michael Colesky u. a. „A Critical Analysis of Privacy Design Strategies“. In: *S&P Workshops*. IEEE, 2016, S. 33–40.

[13] Wolfgang Däubler. „Die kontrollierten Belegschaften“. In: *Datenschutz – Grundlagen, Entwicklungen und Kontroversen*. Hrsg. von Jan-Hinrik Schmidt und Thilo Weichert. bpb, Bonn, 2012.

[14] Deutscher Bundesrat. *Empfehlungen der Ausschüsse zu Punkt 36 der 954. Sitzung des Bundesrates am 10. März 2017 – Entwurf eines Gesetzes zur Anpassung des Datenschutz- rechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), BR-Drucksache 110/1/17*. 2017.

[15] Deutscher Bundestag. *Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz- Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), Drucksache 18/11325*. 2017.

[16] Düsseldorfer Kreis. *Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 23./24. April 2009 in Schwerin – Beschluss des Düsseldorfer Kreises vom 24. April 2009, Datenschutzrechtliche Aspekte des Mitarbeiter-Screenings in international tätigen Unternehmen*. 2009.

[17] Düsseldorfer Kreis. *Orientierungshilfe zu den Datenschutz- anforderungen an App-Entwickler und App-Anbieter, Stand 16. Juni 2014*. 2014.

[18] Cynthia Dwork u. a. „The algorithmic foundations of differential privacy“. In: *Foundations and Trends in Theoretical Computer Science* 9.3–4 (2014), S. 211–407.

[19] eazyBI. *Git Commit Log Analysis Made Easy*. URL: https://eazybi.com/integrations/git.

[20] *Eclipse Mylyn*. URL: http://www.eclipse.org/mylyn/.

[21] Eugen Ehmann und Martin Selmyr, Hrsg. *DS-GVO – Datenschutz-Grundverordnung – Kommentar*. C.H. Beck, München, 2017.

[22] Finanzministerium des Landes Schleswig-Holstein, DBB Beamtenbund, Tarifunion Landesbund Schleswig-Holstein, Deutscher Gewerkschaftsbund Bezirk Nord. *Richtlinie zur Nutzung von Internet und E-Mail – Vereinbarung nach § 59 Mitbestimmungsgesetz des Landes Schleswig-Holstein (MBG)*. 2005.

[23] *Gerrit*. URL: https://www.gerritcodereview.com.

[24] Siavash Ghiasvand und Florina M. Ciorba. „Anonymization of System Logs for Privacy and Storage Benefits“. In: *CoRR* abs/1706.04337 (2017).

[25] Github. *Removing sensitive data from a repository*. URL: https://help.github.com/articles/removing-sensitive-data-from-a-repository/.

[26] *Happyfox*. URL: http://www.happyfox.com/.

[27] Dominik Herrmann. „Beobachtungsmöglichkeiten im Domain Name System: Angriffe auf die Privatsphäre und Techniken zum Selbstdatenschutz“. In: *Ausgezeichnete Informatikdissertationen 2014*. Hrsg. von Steffen Hölldobler. Bd. D-15. LNI. GI, 2014, S. 91–100.

[28] Dominik Herrmann. „Unerfreulich auskunftsfreudig: Inferenzangriffe auf DNS-Anfragen bedrohen unsere Privatsphäre“. In: *Datenbank-Spektrum* 16.2 (2016), S. 119–126.

[29] Dominik Herrmann u. a. „Behavior-based tracking of Internet users with semi-supervised learning“. In: *14th Annual Conference on Privacy, Security and Trust, PST 2016, Auckland, New Zealand, December 12-14, 2016*. IEEE, 2016, S. 596–599.

[30] Dominik Herrmann u. a. „EncDNS: A Lightweight Privacy-Preserving Name Resolution Service“. In: *Computer Security - ESORICS 2014 - 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part I*. Hrsg. von Miroslaw Kutylowski und Jaideep Vaidya. Bd. 8712. Lecture Notes in Computer Science. Springer, 2014, S. 37–55.

[31] S. Hockling. *Big Data: Der Arbeitsplatz misst Tastaturanschlag und Puls*. 2015. URL: https://www.zeit.de/karriere/beruf/2015-11/big-data-mitarbeiter-ueberwachung-people-analytics.

[32] Susan Hohenberger u. a. „ANONIZE: A Large-Scale Anonymous Survey System“. In: *IACR Cryptology ePrint Archive* 2015 (2015), S. 681.

[33] *Icinga – Open Source Monitoring*. URL: https://www.icinga.com.

[34] A. Ju u. a. „Teamscope: Scalable Team Evaluation via Automated Metric Mining for Communication, Organization, Execution, and Evolution“. In: *Learning @ Scale*. ACM, 2017, S. 249–252.

[35] T. Kemp. *Big Data für die Mitarbeiter-Optimierung: Der Quantified Workplace – Pest oder Paradies?* 13.04.2014. URL: https://t3n.de/news/quantified-workplace-big-data-539607/ (besucht am 28. 07. 2017).

[36] Matthias Kirchler u. a. „Tracked Without a Trace: Linking Sessions of Users by Unsupervised Learning of Patterns in Their DNS Traffic“. In: *Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security, AISec@CCS 2016, Vienna, Austria, October 28, 2016*. Hrsg. von David Mandell Freeman, Aikaterini Mitrokotsa und Arunesh Sinha. ACM, 2016, S. 23–34.

[37] 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. März in Hamburg. *Beschäftigten- datenschutzgesetz jetzt! – Entschließung Stand: 27. März 2014*. 2014.

[38] Jürgen Kühling und Benedikt Buchner, Hrsg. *Datenschutzgrundverordnung – Kommentar*. C.H. Beck, München, 2017.

[39] Dong Lin u. a. „Scalable and Anonymous Group Communication with MTor“. In: *PoPETs* 2016.2 (2016), S. 22–39.

[40] Patrick Lincoln u. a. „Privacy-Preserving Sharing and Correlation of Security Alerts“. In: *USENIX Security Symposium*. USENIX, 2004, S. 239–254.

[41] Wouter Lueks u. a. „Revocable Privacy: Principles, Use Cases, and Technologies“. In: *APF*. Bd. 9484. LNCS. Springer, 2015, S. 124–143.

[42] Mika Mäntylä u. a. „Mining valence, arousal, and dominance: possibilities for detecting burnout and productivity?“ In: *MSR*. ACM, 2016, S. 247–258.

[43] Markets and Markets. *Log Management Market worth 1248.9 Million USD by 2022*. 2017. URL: https://www.marketsandmarkets.com/PressReleases/log-management.asp.

[44] Matthias Marx u. a. „Hashing of personally identifiable information is not sufficient“. In: *SICHERHEIT 2018*. Hrsg. von Hanno Langweg u. a. Bonn: Gesellschaft für Informatik e.V., 2018, S. 55–68.

[45] Mattermost Jira. *PLT-45: Spec OTR v2 messaging*. 2015. URL: http://t1p.de/osco.

[46] Mattermost Product Feedback. *Off The Record messaging*. 2016. URL: http://t1p.de/ub9v.

[47] M. H. D. d. Moura u. a. „Extracting New Metrics from Version Control System for the Comparison of Software Developers“. In: *Brazilian Symposium on Softw. Engineering*. 2014, S. 41–50.

[48] Günter Müller und Andreas Pfitzmann, Hrsg. *Mehrseitige Sicherheit in der Kommunikationstechnik*. Addison-Wesley, 1997.

[49] Gail C. Murphy u. a. „How Are Java Software Developers Using the Eclipse IDE?“ In: *IEEE Software* 23.4 (2006), S. 76–83.

[50] neo4J. *KeyLines: Graphing GitHub*. URL: https://neo4j.com/blog/keylines-graphing-github/.

[51] S. Onoue u. a. „A Study of the Characteristics of Developers' Activities in GitHub“. In: *APSEC*. Bd. 2. IEEE, 2013, S. 7–12.

[52] Alen Peacock, Xian Ke und Matthew Wilkerson. „Typing patterns: A key to user identification“. In: *IEEE Security & Privacy* 2.5 (2004), S. 40–47.

[53] Roel Peeters u. a. „Enhancing Transparency with Distributed Privacy-Preserving Logging“. In: *ISSE*. Springer, 2013, S. 61–71.

[54] Persistance Market Research. *Global IT Infrastructure Monitoring Market is Expected to be Valued at US$ 34.1 Bn by 2024*. 2016. URL: https://www.persistencemarketresearch.com/mediarelease/it-infrastructure-monitoring-market.asp.

[55] D. Radcliffe. *What does your GitHub Punch-Card Graph say about You?* URL: https://medium.com/@deaniusaur/what-does-your-github-punch-card-graph-say-about-you-7d2ad7896f6d (besucht am 27. 07. 2017).

[56] Ayushi Rastogi u. a. „Samiksha: mining issue tracking system for contribution and performance assessment“. In: *ISEC*. ACM, 2013, S. 13–22.

[57] Ayushi Rastogi und Nachiappan Nagappan. „On the Personality Traits of GitHub Contributors“. In: *ISSRE*. IEEE, 2016, S. 77–86.

[58] C. Reindl und S. Krügl. „People Analytics: Big Data im Personalwesen“. In: *t3n* 41 (2015), S. 72–75.

[59] Gregorio Robles u. a. „Developer identification methods for integrated data from various sources“. In: *ACM SIGSOFT Software Engineering Notes* 30.4 (2005), S. 1–5.

[60] *Rocket.Chat*. URL: https://rocket.chat.

[61] *Tuleap*. URL: https://www.tuleap.org/.

[62] Nik Unger u. a. „SoK: Secure Messaging“. In: *Security and Privacy*. IEEE, 2015, S. 232–249.

[63] Rahul Venkataramani u. a. „Discovery of technical expertise from open source code repositories“. In: *WWW*. ACM, 2013.

[64] A. Yust. *GitHub for recruiters*. URL: https://medium.com/@aiiane/github-for-recruiters-66868c57c79a.