

FORSCHUNGSREPORT

Daten – Innovation – Privatheit

Mit Inverser Transparenz
das Gestaltungsdilemma
der digitalen Arbeitswelt lösen

ANDREAS BOES, THOMAS HESS, ALEXANDER PRETSCHNER, TOBIAS KÄMPF, ELISABETH VOGL (HRSG.)

Der Forschungsreport ist im Rahmen des BMBF-Projekts „Inverse Transparenz. Beteiligungsorientierte Ansätze für Datensouveränität in der digitalen Arbeitswelt gestalten“ entstanden. Das interdisziplinäre Verbundprojekt wird vom ISF München geleitet und in enger Zusammenarbeit mit der Technischen Universität München (TUM), der Ludwig-Maximilians-Universität München (LMU) und der Software AG umgesetzt. Es wird im Rahmen der Ausschreibung „Privatheit und informationelle Selbstbestimmung in der digitalen Arbeitswelt“ durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert und vom Projektträger VDI/VDE Innovation + Technik GmbH betreut (Laufzeit: November 2018 bis Juli 2022). Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Herausgebern.

Weitere Informationen:

<https://www.inversetransparenz.de/>

EDITORIAL

Daten durchdringen die Welt und (fast) alles, was wir tun. Im gleichen Maße, wie die Digitalisierung voranschreitet, wird unser Handeln immer transparenter. Auf der einen Seite öffnen sich damit neue Möglichkeiten, um Innovationen zum Wohle der Gesellschaft zu schaffen und die Modernisierung von Wirtschaft und Arbeitswelt voranzutreiben. Auf der anderen Seite droht ein dystopisches Szenario, das bestimmt wird von Überwachung und Kontrolle. Wie wir mit Daten und der Transparenz, die sie erzeugen, umgehen, ist also die Schlüsselfrage der digitalen Transformation. In der Informationsökonomie, die mit ihren neuen Wertschöpfungssystemen, Geschäftsmodellen und Arbeitskonzepten von Big Data lebt, hat die Antwort hierauf eine grundlegend strategische Bedeutung.

Im Rahmen unseres interdisziplinären Projekts „Inverse Transparenz: Beteiligungsorientierte Ansätze für Datensouveränität in der digitalen Arbeitswelt gestalten“ verabschieden wir uns von den Schwarz-Weiß-Bildern, die bislang die Diskussion um die Datenökonomie dominiert haben, und vollziehen einen Perspektivenwechsel. Mit Inverser Transparenz denken wir die Stärkung von Datensouveränität und Datenschutz einerseits und die intelligente Nutzung von Daten für digitale Innovation und Wertschöpfung andererseits zusammen. Das Konzept ist ebenso voraussetzungs- voll wie vielversprechend und – mit Blick auf die Corona-Pandemie, in deren Folge die Digitalisierung von Arbeit einen enormen Schub erhalten hat – aktueller denn je.

In den letzten drei Jahren haben wir Inverse Transparenz in der Praxis zur Anwendung gebracht und aus verschiedenen Blickwinkeln wissenschaftlich erforscht. Unsere Befunde – entstanden im Rahmen eines betrieblichen Praxislaboratoriums bei der Software AG – zeigen: Inverse Transparenz ist machbar und hat das Potenzial, neue datenbasierte Innovationskulturen zu etablieren und das Empowerment der Beschäftigten zu fördern.

Die Ergebnisse unseres gemeinsamen Forschens, Experimentierens und Gestaltens haben wir in diesem Forschungsreport für Sie aufbereitet. Er analysiert Inverse Transparenz aus Sicht der Soziologie, Informatik, Wirtschaftsinformatik und Rechtswissenschaft und lässt die Arbeit eines außergewöhnlichen Praxislaboratoriums Revue passieren. Namhafte Expertinnen und Experten aus Wirtschaft, Politik und Interessenvertretung kommen mit ihren Impulsen zur Zukunft der Datenökonomie ebenso zu Wort wie die Initiatoren dieses Leuchtturmprojekts.

Wir haben an dieser Stelle vielen zu danken: Zuallererst danken wir dem Bundesministerium für Bildung und Forschung (BMBF), ohne dessen Förderung das Verbundvorhaben nicht umsetzbar gewesen wäre. Zudem danken wir unseren Verbundpartnern – der Software AG, der Technischen Universität München (TUM) und der Ludwig-Maximilians-Universität München (LMU) – für die exzellente Zusammenarbeit. Durch das enge Zusammenwirken der Verbundpartner und das außerordentliche Engagement der Mitarbeiterinnen und Mitarbeiter der Software AG ist es gelungen, aus einem abstrakten Konzept ein praxistaugliches Gestaltungsinstrument zu machen. Und nicht zuletzt geht unser Dank an jene Akteure und Akteurinnen aus unserem Netzwerk, die das Projekt mit ihrer Expertise unterstützt haben und ihre Impulse für eine nachhaltige Gestaltung der digitalen Arbeitswelt mit uns geteilt haben.

Wir wünschen eine spannende Lektüre.

INHALT

Einführung

6 GELEITWORT

Auch im Digitalen ist Vertrauen
unbezahlbar

8 INTERVIEW

Datennutzung und Datenschutz
nach vorne denken

14 ANALYSE

Transparenz in der digitalen
Arbeitswelt

Berichte aus der Forschung

24 SOZIOLOGIE

Inverse Transparenz – ein neuer Gestaltungs-
ansatz für die Arbeitswelt?

36 MANAGEMENTFORSCHUNG

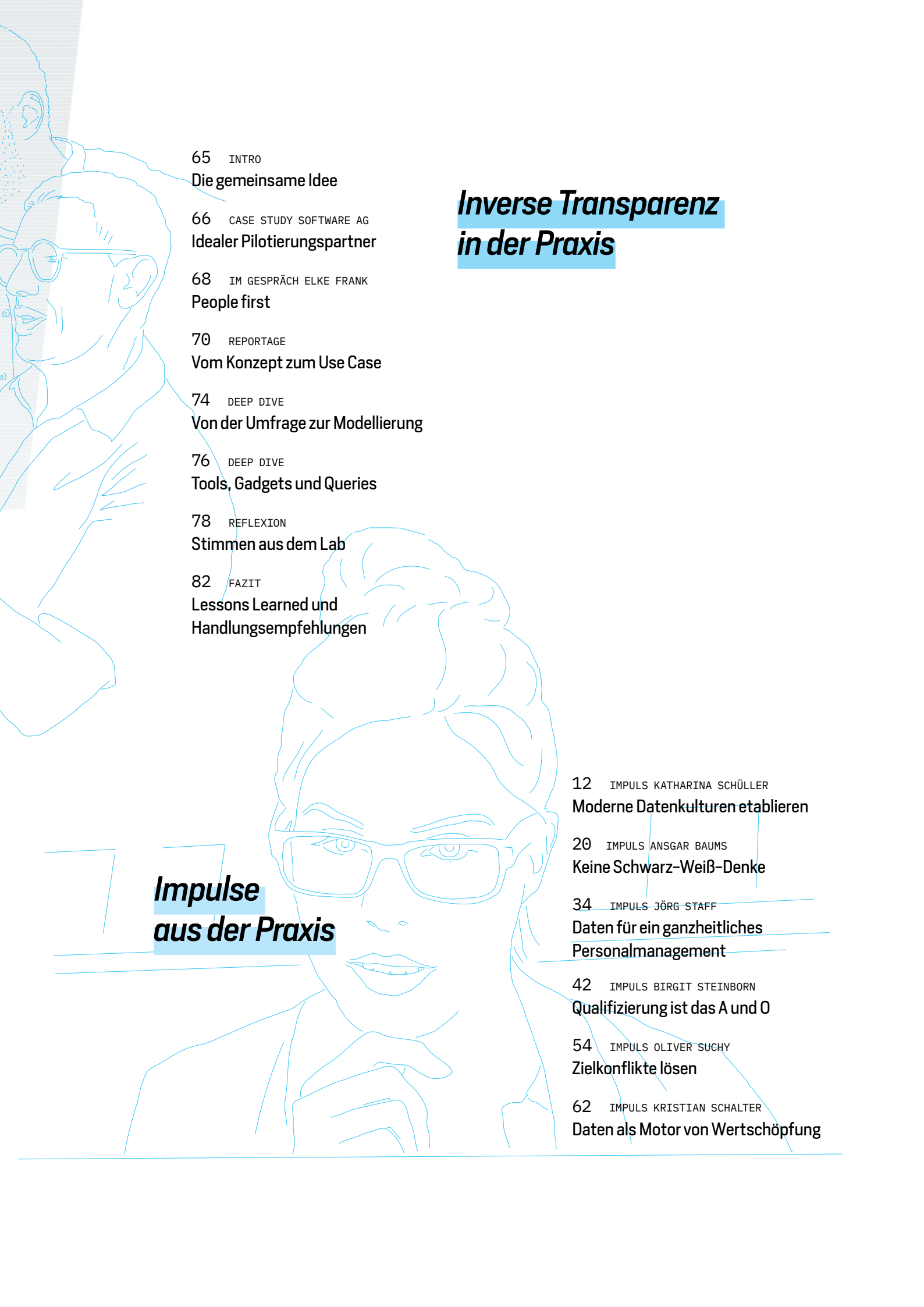
Datafizierung am Arbeitsplatz

44 INFORMATIK

Transparency by Design

56 RECHTSWISSENSCHAFT

Informationelle Selbstbestimmung in der
digitalen Arbeitswelt



Inverse Transparenz in der Praxis

65 INTRO

Die gemeinsame Idee

66 CASE STUDY SOFTWARE AG

Idealer Pilotierungspartner

68 IM GESPRÄCH ELKE FRANK

People first

70 REPORTAGE

Vom Konzept zum Use Case

74 DEEP DIVE

Von der Umfrage zur Modellierung

76 DEEP DIVE

Tools, Gadgets und Queries

78 REFLEXION

Stimmen aus dem Lab

82 FAZIT

**Lessons Learned und
Handlungsempfehlungen**

**Impulse
aus der Praxis**

12 IMPULS KATHARINA SCHÜLLER

Moderne Datenkulturen etablieren

20 IMPULS ANSGAR BAUMS

Keine Schwarz-Weiß-Denke

34 IMPULS JÖRG STAFF

**Daten für ein ganzheitliches
Personalmanagement**

42 IMPULS BIRGIT STEINBORN

Qualifizierung ist das A und O

54 IMPULS OLIVER SUCHY

Zielkonflikte lösen

62 IMPULS KRISTIAN SCHALTER

Daten als Motor von Wertschöpfung

Datafizierung am Arbeitsplatz

Inverse Transparenz
als Enabler für neue
Führungskonzepte

THOMAS HESS,
RAHILD NEUBURGER,
MAREN GIERLICH-JOAS,
INSTITUT FÜR DIGITALES MANAGEMENT UND
NEUE MEDIEN AN DER LMU MÜNCHEN

Führungskräfte sehen sich im digitalen Zeitalter mit den Chancen und den Herausforderungen steigender Transparenz am Arbeitsplatz konfrontiert. Während direkte, einseitige Transparenz zu Informationsasymmetrien und Misstrauen zwischen Mitarbeitenden und Führungskräften führt, bietet der Ansatz der Inversen Transparenz eine Basis für innovative Führungskonzepte. Wir beschreiben das Spannungsfeld der steigenden Transparenz in der Personalführung, leiten Inverse Transparenz als mögliche Lösung ab und zeigen Implikationen auf.

37

1_ Spannungsfelder in der Personalführung durch steigende Datenverfügbarkeit

Der bereits thematisierte technologische Wandel zeigt sich – bezogen auf die Arbeitswelt – insbesondere im Bereich der Personalführung. In den vergangenen Jahrzehnten erfuhren digitale Tools am Arbeitsplatz immer weitere Verbreitung. Bereits in den 1960er Jahren wurden erste Payroll-Systeme zur Automatisierung von Gehaltszahlungen verwendet. Diese ersten Systeme dienten der Unterstützung operativer HR-Prozesse (siehe Johnson et al.⁹). In den kommenden Jahrzehnten entwickelten sich diese Systeme weiter zu Entscheidungsunterstützungs-Tools und sogenannten People-Analytics-Informationssystemen im HR-Bereich, die strategische Aufgaben unterstützen können und über die rein deskriptive Analyse hinausgehen. Mittlerweile können People Analytics oft auf der Basis von künstlicher Intelligenz Vorhersagen über zukünftig oder jetzt benötigte Profile von Mitarbeitenden treffen und Handlungsempfehlungen zur Zusammenstellung und Führung von Teams ableiten (siehe Gal et al.⁴). Neben dem Funktionsumfang dieser Tools steigt auch ihre Verbreitung und viele

Unternehmen führen Positionen wie den „Head of People Analytics“ ein, wodurch die Datenzentriertheit von HR-Abteilungen nochmals unterstrichen wird.

Diese von Daten durchdrungenen Arbeitsplätze bergen sowohl Chancen als auch Risiken für Mitarbeitende und Management. Die Vorteile von Tools wie People Analytics liegen aus Sicht der Arbeitgeber in einer gesteigerten Transparenz jeglicher Prozesse am Arbeitsplatz und der Möglichkeit, Prozesse effizienter zu gestalten. Für Mitarbeitende bieten sie die Chance, selbstbestimmt zu arbeiten und sich vor Überlastung zu schützen, sofern sie Einblicke in die Daten erhalten. Jedoch besteht die Gefahr, dass Arbeit zu stark quantifiziert wird, sich Manager und Managerinnen nicht mehr auf ihr Erfahrungswissen verlassen und die Privatsphäre der Arbeitnehmerinnen und Arbeitnehmer untergraben wird (siehe Gierlich-Joas et al.⁶). Das folgende Fallbeispiel von Microsoft zeigt die Chancen und Risiken dieser Tools anschaulich auf.

Fallbeispiel: Microsoft Productivity Scores

Viele Unternehmen setzen zur Kommunikation und zum kollaborativen Arbeiten Microsoft-Produkte ein. Microsoft bietet zahlreiche Möglichkeiten an, die in den Systemen anfallenden Daten zu analysieren und sichtbar zu machen. Ein Ansatz dazu waren die im Oktober 2020 vorgestellten „Microsoft Productivity Scores“. In den Scores flossen zahlreiche Daten zusammen, beispielsweise zur Häufigkeit der Teilnahme an MS-Teams-Meetings wie auch der aktiven Beteiligung in Meetings. Insbesondere in Deutschland traf diese Idee auf starke Kritik und die Süddeutsche Zeitung titelte: „Angestellte überwachen? Microsoft macht's möglich“ (siehe Hurtz⁸). Wenige Wochen nach der Einführung musste Microsoft die Scores wieder zurücknehmen („Microsoft rudert nach Datenschutzskandal zurück“, siehe Popiolek¹⁵).

Von der Idee, Daten von Beschäftigten am Arbeitsplatz nutzbar zu machen, getrieben, entwickelte Microsoft daraufhin

die „Employee-Experience-Plattform Viva“. Im Gegensatz zu den Productivity Scores können sich Mitarbeitende hier vernetzen und es stehen Themen wie Empowerment zu ihrer Selbstorganisation im Vordergrund. Das Ziel bei Viva ist nicht die direkte, eindimensionale Transparenz zwischen Führungskräften und Mitarbeitenden, sondern die beidseitige Transparenz, auch unter Teamkollegen und -kolleginnen. Dies bietet gerade in Zeiten von Remote Work die Möglichkeit, räumliche und zeitliche Grenzen zwischen Beschäftigten zu überbrücken. Viva wurde im Gegensatz zu den Productivity Scores deutlich besser angenommen und Zeitschriften lobten „Microsoft Viva für ein neues und besseres Mitarbeiter-Erlebnis“ (siehe Weiß¹⁶). Dieses Beispiel zeigt sowohl die Gefahr von herkömmlichen Transparenz-Tools als auch die Potenziale von Systemen, die auf dem Prinzip der Inversen Transparenz basieren.

2_ Inverse Transparenz als Basis für neue Führungskonzepte

38

2.1_ Was bedeuten Führung und Management?

Um die Implikationen von Inverser Transparenz auf Personalführung zu verstehen, muss der Begriff der „Führung“ zuerst definiert werden. Es gibt nicht die eine universale Definition von Führung. Gemeinsam haben viele Definitionsversuche, dass Führung darauf zielt, Individuen so zu beeinflussen, dass sie sich zum Wohl der Gruppe verhalten und die Ziele des Unternehmens verfolgen (siehe Kaiser¹⁰). Demnach benötigt die führende Person „die Fähigkeit [...], andere zu beeinflussen, zu motivieren und zu befähigen, zur Effektivität und zum Erfolg der Organisationen beizutragen, denen sie angehören“ (House et al. 7, 5).

Die Begriffe „Führung“ und „Management“ werden oftmals synonym verwendet. Sie unterscheiden sich jedoch und lassen sich entlang der Dimensionen Ressourcen, Menschen und Kontrolle differenzieren (siehe Kotter¹¹). Die Grundannahme bei Führung ist, dass sie Wandel und Bewegung erzeugt und dabei eine Vision entwickelt, Menschen zusammenführt, motiviert und inspiriert (siehe Liphadzi et al.¹²). Beim Management liegt der Fokus auf Organisieren und dem Erzielen von Konsistenz. Aufgaben eines Managers umfassen daher die Planung und Budgetierung, das Controlling von Prozessen und Ressourcen sowie das Besetzen von Stellen (Liphadzi et al.¹²).

Auch wenn beide Konzepte eng verwandt sind, beschäftigen wir uns beim Konzept der Inversen Transparenz primär mit dem menschenorientierten Begriff der Führung. Dennoch hat Inverse Transparenz als holistisches Konzept auch Auswirkungen auf Managementaufgaben.

2.2_ Neue Anforderungen an Führung im digitalen Zeitalter

Der Begriff der Führung hat eine lange Tradition im Bereich der Geistes- und Sozialwissenschaften. Während Führungstheorien Führungs-Phänomene abstrakt beschreiben, gibt es in der Literatur zahlreiche Führungskonzepte, die diese Theorien auf die Praxis herunterbrechen. Neue Anforderungen an die Führung spiegeln sich daher in neuen Führungstheorien und Führungskonzepten wider.

Lange Zeit betrachtete man Führung unter dem Aspekt der sogenannten Eigenschaftstheorie, die nach den zugrundeliegenden Charakteristika der Führungskraft unterschiedet. Dem Charisma der Führungsperson wurde dabei eine besondere Bedeutung zugesprochen. In den 1970er und 1980er Jahren wurde diese Betrachtungsweise um die Bedürfnisse und Eigenschaften der Mitarbeitenden erweitert, was als transaktionale und

transformationale Führung verstanden wird. Mitarbeitende sollen demnach unter Berücksichtigung ihrer Motivation und ihres Könnens individuell gefördert werden. Zuletzt wurden moderne Ansätze wie die E-Leadership oder dezentrale Führungskonzepte diskutiert, bei denen verstärkt auf die Nutzung digitaler Technologien zur Führung, die Verteilung von Verantwortung wie auch die Partizipation der Mitarbeitenden in Führungsentscheidungen eingegangen wird (siehe Dinh et al.¹).

Ein beliebtes Tool einer derartigen Bottom-up-Führung stellt der Ansatz Objectives & Key Results (OKR) dar. Im Gegensatz zum klassischen „Management by Objectives“ basiert hier die Setzung von Zielen auch auf von den Mitarbeitenden gesetzten Zielen (objectives) sowie auf messbaren Ergebnissen (key results). Der Weg zur Zielerreichung ist dabei den Mitarbeitenden freigestellt. Die OKR-Methode setzt auf große Transparenz und Integration von Mitarbeitenden. Eingeführt wurde sie 1999 erstmals von John Doerr bei Google (siehe Doerr²).

Top-down-Führungskonzepte werden dem Wunsch nach selbstbestimmtem Arbeiten nicht gerecht.

Die bisherige Literatur bietet jedoch wenig Ansatzpunkte, wie Daten aus Arbeitsprozessen als Grundlage für innovative Führungskonzepte genutzt werden können. Ansätze wie „data-driven leadership“ stecken noch in den Kinderschuhen. Zudem werden traditionelle Top-down-Führungskonzepte dem wachsenden Wunsch jüngerer Beschäftigten-Generationen nach selbstbestimmtem Arbeiten nicht mehr gerecht. So hat eine Umfrage bei Experten und Expertinnen aus Industrie und Wissenschaft ergeben, dass Empowerment und der Umgang mit steigender Transparenz am Arbeitsplatz als die größten zukünftigen Herausforderungen von Führungskräften wahrgenommen werden (siehe Gierlich-Joas⁵). Oftmals werden Bedenken geäußert, wie Transparenz gegenüber Mitarbeitenden geschaffen werden kann, ohne dass diese überfordert werden. Das Konzept „Empowerment“ erfreute sich grundsätzlich großer Beliebtheit, doch die konkrete Umsetzung in der Praxis wurde als problematisch empfunden, da Verantwortlichkeiten aufgeweicht werden und die Rolle der Führungskraft neu zu definieren ist (siehe Gierlich-Joas⁵).

Wir stellen uns daher die Frage: Wie kann Führung – das Beeinflussen von Individuen, sodass sich diese zum Wohl des Unternehmens verhalten – im digitalen Zeitalter und bei steigender direkter Transparenz gestaltet werden?

2.3_ Inverse Transparenz als Basis für neue Führungskonzepte

Das Konzept der Inversen Transparenz versucht das Spannungsfeld zwischen Empowerment und Überwachung am Arbeitsplatz zu lösen und legt die Grundlage für innovative Führungskonzepte. Es geht nicht darum, Daten für Leistungs- und Performancemessung zu nutzen, sondern nachhaltige Wege aufzuzeigen, die ohnehin vorhandenen Daten im Sinne der Mitarbeiterin oder des Mitarbeiters zu nutzen.

Die Führungsbeziehung zwischen Manager bzw. Managerin und Mitarbeitenden ist in der Regel von Informationsasymmetrien geprägt. Zum einen verfügen Führungskräfte oft nicht über genauere Einblicke in die Arbeit ihrer Mitarbeitenden. Zum anderen ist es für Beschäftigte weitgehend intransparent, welche Daten über die eigenen Arbeitsprozesse existieren und wer diese Daten für welche Zwecke nutzt. Den Annahmen der Prinzipal-Agenten-Theorie folgend, signalisieren daher Mitarbeitende, welche Arbeitsschritte sie durchführen, und Führungskräfte investieren in Überwachungsaktivitäten (siehe Eisenhardt³; Picot & Neuburger⁴). Dieses traditionelle Setting führt nicht nur zu vermeidbaren Agency-Kosten, sondern häufig auch zu Misstrauen und Ineffizienzen sowohl bei Führungskräften wie auch bei Beschäftigten.

Werden die Arbeitsdaten der Mitarbeitenden dagegen im Sinne der Inversen Transparenz geteilt, so kann unter bestimmten Voraussetzungen, auf die später noch eingegangen wird, eine Demokratisierung von Macht stattfinden. Mitarbeitende und Führungskräfte verfügen über dieselben Daten und können damit auf Augenhöhe miteinander kommunizieren. Gleichzeitig gibt die Führungskraft Verantwortung an die Beschäftigten beziehungsweise an das Team ab und befähigt dadurch zum selbstorganisierten Arbeiten. Tägliche Aufgaben müssen nun nicht mehr engmaschig überwacht werden, sondern das Team kann sich eigenverantwortlich um diese kümmern, da die hierfür benötigten Daten zur Verfügung stehen. Mitarbeitende gewinnen durch diesen Ansatz an Verhandlungsmacht, da sie sich besser vor Überlastung schützen können und Management-Entscheidungen offengelegt werden. Gleichzeitig werden sie in die Lage versetzt, sich auf der Basis der Daten selbst weiterzuentwickeln und zu verbessern. Durch Führungskonzepte, die auf dem Prinzip der Inversen Transparenz fußen, entstehen Führungsbeziehungen, die sich auf Vertrauen, Transparenz, Selbstorganisation und Empowerment begründen (siehe Abbildung 1). Damit unterscheiden sie sich von dem klassischen Prinzipal-Agenten-Denken.

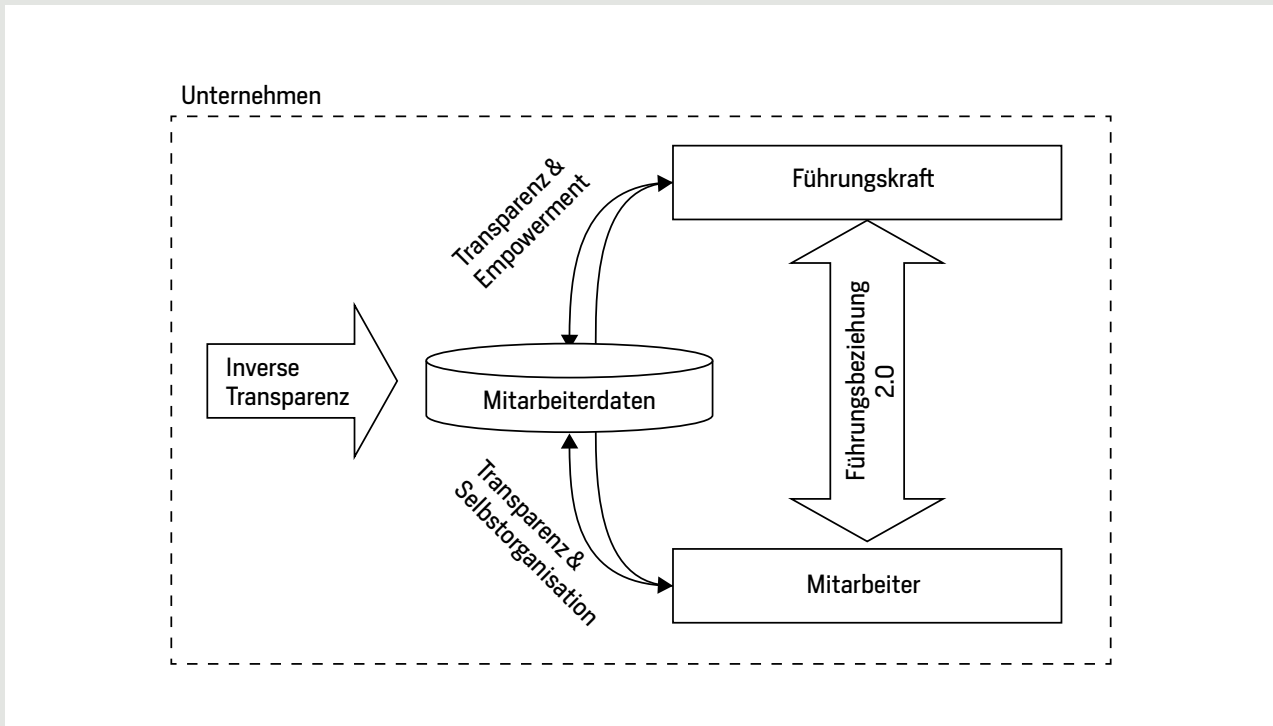


Abbildung 1. Führungsbeziehungen 2.0 auf der Basis von Inverser Transparenz (eigene Darstellung)

40

3_ Fazit: Zentrale Gestaltungsfelder

Das Konzept der Inversen Transparenz bietet aus Sicht der Führung und damit letztlich auch des Managements große Potenziale, um den wachsenden Spannungen zwischen Selbstorganisation/Empowerment und Überwachung zu begegnen und Daten von Mitarbeitern und Mitarbeiterinnen nachhaltig nutzbar zu machen. Bisherige Führungskonzepte stoßen hier an ihre Grenzen. Die Notwendigkeit für Unternehmen aller Branchen, auf innovative Führung zu setzen, wird vor dem Hintergrund des angesprochenen Wertewandels wie auch des gegenwärtig zu beobachtenden Fachkräftemangels noch einmal verschärft.

Jedoch sollte die konkrete Ausgestaltung des Konzepts der Inversen Transparenz sorgfältig an die jeweiligen Rahmenbedingungen im Unternehmen angepasst werden, denn ein sinnvoller „One-size-fits-all“-Ansatz, der in jedem Unternehmen unabhängig von Art und Größe umsetzbar ist, lässt sich gegenwärtig nicht erkennen. Zudem sollte das Konzept der Inversen Transparenz nicht zu einer Strategie im Sinne von: „Je mehr Transparenz, desto besser“ führen, da zu viele Daten

auch zu Ineffizienzen insbesondere durch eine Informationsüberflutung führen können. Der optimale Grad der Inversen Transparenz sollte daher unternehmensspezifisch zwischen Führungskräften und Beschäftigten beziehungsweise Teams in den jeweiligen Unternehmen ausgehandelt werden.

Insbesondere erfordert die Integration von Inverser Transparenz in Unternehmen ein offenes Mindset auf Seiten der Mitarbeitenden und der Führungskräfte; aber auch auf Seiten der HR-Abteilungen und des Betriebsrats. Zudem lässt sich Inverse Transparenz nur auf Basis einer entsprechenden Vertrauenskultur realisieren. Auf diese und weitere Rahmenbedingungen und Gestaltungsfelder gehen wir zum Abschluss des Berichts detaillierter ein.

Aus der Perspektive der Führung ergeben sich dabei vor allem folgende Handlungsfelder und offene Fragestellungen:

- Welche Anforderungen stellen sich an Führungskräfte konkret?
- Wie lassen sich Datenerhebung und datenbasierte Entscheidungen transparent gestalten und kommunizieren?

- Welche Rolle nehmen der Betriebsrat und die HR-Abteilung bei der Implementierung von Inverser Transparenz ein?
- Wie lässt sich der optimale Grad an Inverser Transparenz darstellen und wie wird dieser zwischen allen Beteiligten im Unternehmen ausgehandelt?
- Welche Rahmenbedingungen und Stellschrauben lassen sich in Unternehmen erkennen, die Inverse Transparenz fördern?

4_ Referenzen

- 1 Dinh, J. E., Lord, R. G., Gardner, W. L., Meuser, J. D., Liden, R. C., Hu, J. Leadership theory and research in the new millennium: Current theoretical trends and changing perspectives. *The Leadership Quarterly* 25, 1 (2014), 36–62.
- 2 Doerr, J. *OKR. Objectives & Key Results: Wie Sie Ziele, auf die es wirklich ankommt, entwickeln, messen und umsetzen*. Franz Vahlen, 2018.
- 3 Eisenhardt, K. M. Agency Theory: An Assessment and Review. *Academy of Management Review* 14, 1 (1989), 57–74.
- 4 Gal, U., Blegind Jensen, T., Stein, M.-K. People Analytics in the Age of Big Data: An Agenda for IS Research. In *Proceedings International Conference on Information Systems 2017*, Atlanta.
- 5 Gierlich-Joas, M. Identifying and Overcoming Future Challenges in Leadership: The Role of IS in Facilitating Empowerment. In *Tagungsband 16. Internationale Tagung Wirtschaftsinformatik, Duisburg-Essen, 9.–11. März 2021*.
- 6 Gierlich-Joas, M., Hess, T., Neuburger, R. More Self-Organization, More Control – Or Even Both? Inverse Transparency As A New Digital Leadership Concept. *Business Research* 13 (2020), 921–947.
- 7 House, R. J., Hanges, P. J., Javidan, M., & Dorfman, P. W. Understanding cultures and implicit leadership theories across the globe: An introduction to project GLOBE. *Journal of World Business* 37 (2002), 3–10.
- 8 Hurtz, S. Angestellte überwachen? Microsoft macht's möglich. *Süddeutsche Zeitung*, 27.11.2020. <https://www.sueddeutsche.de/digital/microsoft-productivity-score-ueberwachung-arbeitsplatz-1.5130228>.
- 9 Johnson, R. D., Lukaszewski, K. M., Stone, D. L. The Evolution of the Field of Human Resource Information Systems: Co-Evolution of Technology and HR Processes. In *Communications of the ACM* 38 (2016), 533–553.
- 10 Kaiser, R. B. The leadership value chain. *The Psychologist Manager* 13 (2005), 3, 164–183.
- 11 Kotter, J. P. What leaders really do. *Harvard Business Review* 79, 11, 85–97.
- 12 Liphadzi, M., Aigbavboa, C. O., Thwala, W. D. A Theoretical Perspective on the Difference between Leadership and Management. In *Procedia Engineering* 196 (2017), 478–482.
- 13 Münchner Kreis. *Innovationsfelder der digitalen Welt – Bedürfnisse von übermorgen*. Zukunftsstudie Münchner Kreis, Band V. München, 2013.
- 14 Picot, A., Neuburger, R. Agency-Theorie und Führung. In Kieser A., Reber, G., Wunderer, R. (Hrsg.), *Handwörterbuch der Führung*. Poeschel, 1995, 14–21.
- 15 Popiolek, H. Microsoft rudert nach Datenschutzskandal zurück. *Computerbild*, 2.12.2020. <https://www.computerbild.de/artikel/cb-News-Software-Microsoft-Productivity-Score-29362393.html>.
- 16 Weiß, E.-M. Microsoft Viva für ein neues und besseres Mitarbeiter-Erlebnis. *Heise*, 5.2.2021. <https://www.heise.de/news/Microsoft-Viva-fuer-ein-neues-und-besseres-Mitarbeiter-Erlebnis-5047201.html>.



*Interview mit Birgit Steinborn,
Vorsitzende des Gesamtbetriebsrats
der Siemens AG und stellvertretende
Aufsichtsratsvorsitzende*

»Qualifizierung ist das A und O«

„Mensch vor Marge“. Diesem Leitmotiv hat sich Birgit Steinborn verschrieben. Um die Belegschaft in der Transformation von Siemens zum Digitalkonzern mitzunehmen, setzt sie vor allem auf Qualifizierung. Wie man sie beteiligungsorientiert und vorausschauend gestalten kann und wie sich auch Mitbestimmung verändern muss, erklärt die Gesamtbetriebsratsvorsitzende in diesem Interview.

Frau Steinborn, was bedeutet der gegenwärtige Umbruch für die Arbeitswelt der Siemens-Beschäftigten?

Hinter dieser Transformation stehen technologische Veränderungen durch Digitalisierung, die Entwicklung neuer Produkte und Geschäftsmodelle und die Verbindung von Hardware mit Software. Nicht zuletzt geht es auch um Produktivitätssteigerung. Angesichts der enorm steigenden Geschwindigkeit der Veränderungen ist Agilität und Eigenverantwortung gefragt – nicht nur in der Entwicklung, sondern gerade auch in der Produktion und den indirekten Bereichen. Damit ändern sich die Inhalte der Tätigkeiten und die Arbeitsorganisation. Hierfür müssen wir die Beschäftigten

befähigen und dies kann nur gelingen, wenn wir Mitbestimmung neu denken.

Was muss sich verändern?

Wir brauchen mehr Transparenz über Veränderungen, die vor uns liegen, und eine neue Qualität der Mitbestimmung mit mehr Informations- und Initiativrechten sowie einer stärkeren Einbindung in strategische Entscheidungen, die die Arbeitsplätze der Beschäftigten betreffen. Dazu gehören explizit auch Zugriffsrechte des Betriebsrats auf betriebliche Datensysteme. Es greift viel zu kurz, wenn der Arbeitgeber erst am Ende eines Veränderungsprozesses versucht, die Inhalte mit dem Betriebsrat abzuhaken. Entschei-

dend ist vielmehr eine frühzeitige partnerschaftliche Zusammenarbeit, bei der Belegschaft, Betriebsrat und Unternehmen interagieren und auf dasselbe Ziel hinarbeiten. Wir müssen uns gemeinsam auf die neuen Herausforderungen einstellen, damit wir als Gesamtunternehmen in der Digitalökonomie konkurrenzfähig bleiben.

Wie kommen wir dahin? Was ist Ihre Erfahrung?

Das A und O für eine erfolgreiche Transformation ist Qualifizierung. Lange Zeit ist Siemens bei dem Thema auf Sicht gefahren und hat vor allem in Weiterbildungsmaßnahmen investiert, die sich eng an den aktuellen Anforderungen orientieren – zum Beispiel Produktschulungen. Aber Kurse allein reichen nicht. Wir brauchen eine vorausschauende Qualifizierung, die Zukunftstrends adressiert, auch wenn wir nicht ganz genau wissen, wie die Arbeitsplätze der Zukunft im Detail aussehen und wie viele wir davon brauchen. Hierfür haben wir uns als Gesamtbetriebsrat stark gemacht.

Wie haben Sie diese vorausschauende Qualifizierung aufgegleist?

Über ein Fondsmodell. Das Unternehmen stellt zentrale Mittel in einem separaten Topf bereit. Örtliche Betriebsleitungen und Betriebsräte können sich mit ihren gemeinsamen Konzepten darum bewerben und ein paritätisch besetzter Vergabeausschuss entscheidet nach fest vereinbarten Kriterien, welches Projekt gefördert wird. Dafür tauschen sich die Betriebspartner vor Ort darüber aus, wie sich Technologie, Produkte und Geschäftsmodelle verändern und was dies für die Tätigkeiten der Beschäftigten bedeutet. Dieses Fondsmodell hat einen unwahrscheinlichen Schub gebracht und es sind viele Qualifizierungsprojekte entstanden. Die gewonnenen Erfahrungen fließen jetzt in das unternehmensweite Qualifizierungs-Analysemodell NextWork ein.

Wo liegt der Anreiz für die Beschäftigten?

Sie spüren, dass es direkt um sie und ihr Arbeitsumfeld geht und nicht um irgendeine Maßnahme, die am grünen Tisch entworfen wird. Wir beziehen die Menschen an den einzelnen Standorten mit ihren Kompetenzen und Praxiserfahrungen in unsere Überlegungen ein. Denn sie wissen am besten, welche Schritte notwendig sind, um einen Standort konkurrenzfähig zu halten. Darauf wird das Qualifizierungsprogramm ausgerichtet. Aber Veränderung erzeugt auch Verunsicherung, sogar Ängste. Viele fragen sich: Wozu soll ich das noch machen? Was wird von mir verlangt? Schaffe ich das überhaupt? Dem können wir entgegenwirken, wenn wir die Beschäftigten von Anfang an einbinden.

Sichert diese neue Form der Qualifizierung auch Arbeitsplätze?

Ein Arbeitsplatz wird gesichert, wenn ein Unternehmen konkurrenzfähig und innovativ ist. Und diese Konkurrenzfähigkeit hängt ab von gut qualifizierten Beschäftigten, die Innovationen ent-

wickeln oder umsetzen können. Insofern lautet die Antwort: Ja. Andererseits: Die Digitalisierung erleichtert es gerade in der Wissensarbeit, Tätigkeiten zu verlagern. Wir müssen uns also immer fragen, welche Arbeitskräfte treiben welche Innovationen, welche Fähigkeiten brauchen wir in Zukunft dafür, und welche Beschäftigungschancen entstehen in der Folge hier in Deutschland?

Wie gut ist die Belegschaft für die zunehmend digitale Siemens-Welt aufgestellt?

Das ist sehr unterschiedlich. Für die Beschäftigten, die tagtäglich mit digitalen Arbeitsinhalten zu tun haben, ist vieles selbstverständlich. Die anderen sind eher misstrauisch mit Blick auf die Datennutzung und mögliche Überwachungsszenarien. Dazu kommt, dass immer noch ein großer Teil der Beschäftigten in der Produktion nicht einmal einen digitalen Zugang zum Intranet und damit zu vielen Angeboten des Unternehmens hat. Unser Ziel ist es aber, alle – Werkende und Wissensarbeitende – in die digitale Welt zu holen und damit weiter für gute Beschäftigung zu sorgen.

Das Gespräch führte Dr. Jutta Witte

Transparency by Design

Softwaredesign für einen
transparenten Umgang mit
Daten am Arbeitsplatz

ALEXANDER PRETSCHNER,
VALENTIN ZIEGLMEIER,
LEHRSTUHL FÜR SOFTWARE UND SYSTEMS
ENGINEERING AN DER TU MÜNCHEN

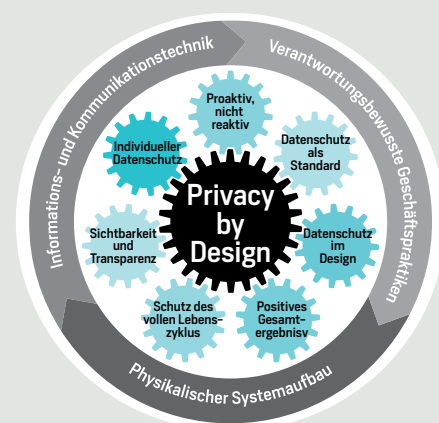
Eine immer transparentere Arbeitswelt erfordert, dass sich Softwaredesign weiterentwickelt, um sinnvolle Anwendungsfälle für Daten zu ermöglichen und zugleich Datenmissbrauch vorzubeugen. Wir beschreiben deshalb Transparency by Design als möglichen Weg für Software am Arbeitsplatz. Dabei blicken wir auf die fundamentalen Veränderungen, die diesen neuen Ansatz notwendig machen, diskutieren mögliche Implikationen für Softwaredesign und erläutern unsere Umsetzung des Konzepts im Rahmen des Forschungsprojekts.

1_ Software im Kontext neuer Transparenz

Daten und die Software, die sie verarbeitet, durchdringen heute alles. Mit der fortschreitenden Digitalisierung wird insbesondere die Arbeitswelt immer transparenter. Diese Realität kreiert zwei zentrale Themen für die Informatik: Auf der einen Seite ergeben sich immense Möglichkeiten, auf Basis von Daten effektivere Software zu gestalten. Prädiktive Analysen, maschinelles Lernen und Big Data ermöglichen komplett neue Anwendungsfälle für Daten. Auf der anderen Seite trägt unsere Disziplin eine klare Verantwortung. Datentransparenz steht erst einmal im Gegensatz zu Datenschutz, welcher einen hohen Stellenwert einnimmt.

Schon im Jahr 1995 schlug Ann Cavoukian, die ehemalige Information and Privacy Commissioner der kanadischen Provinz Ontario, deshalb den Ansatz „Privacy by Design“ vor, welcher im Jahr 2009 in einer Veröffentlichung von sieben fundamentalen Prinzipien konkretisiert wurde (siehe Cavoukian²). Im Gegensatz zur üblichen Vorgehensweise, nach Fertigstellung eines Softwareprojekts den Datenschutz zu

prüfen und gegebenenfalls zu überarbeiten, sieht Privacy by Design vor, Datenschutzgrundsätze von vornherein in die Konzeptionierung und das Design von Software zu integrieren. Dem liegt die Annahme zugrunde, dass sich Softwaredesign grundlegend und inkompatibel verändert, wenn Datenschutz



Privacy by Design (nach Ann Cavoukian)

bewusst einbezogen wird; eine Anpassung, die im Nachhinein nur sehr umständlich oder gar nicht mehr möglich ist.

Cavoukians Sorgen betrafen dabei die legitime Nutzung von Daten innerhalb kontrollierter Systeme. Wie sollte jedoch mit illegitimer Nutzung umgegangen werden? Dazu entwickelte sich zur selben Zeit die Idee der „Information Accountability“, die Daniel Weitzner und Koautoren im Jahr 2007 vorstellten (siehe Weitzner et al.⁷). Ihre informatische Sichtweise bezieht neben der bewusst angedachten Nutzung von Daten deren Missbrauchspotenzial ein. Schon wenn Daten nicht ausreichend gesichert sind, besteht Missbrauchsgefahr, vor allem aber war schon damals bekannt, dass automatisiert abgeleitete Daten und Zusammenführung über mehrere Quellen Risiken bergen. Zugleich betonen die Autoren aber auch ein weiteres Problem des damaligen Status quo: Zu rigide Schutzmaßnahmen schränken legitime Nutzung ein und ersticken Innovation im Keim. Transparenz, als Kernbestandteil von Accountability, kann dann eine eher ermöglichende als problematische Rolle im Datenschutz einnehmen, wenn die Verwendung von Daten beobachtet werden kann und illegitime Nutzung sanktioniert wird.

Gerade am Arbeitsplatz kann die illegitime Nutzung von Daten besondere Schlagkraft gewinnen. Zum Fehlen der Transparenz der Systeme und zur Überforderung der Nutzer kommen die erzwungene Nutzung von Software ohne Wahlmöglichkeit sowie die natürliche Machtasymmetrie zwischen Führungskraft und Mitarbeitenden als Brandbeschleuniger hinzu. Es reicht hier also nicht mehr, die Entscheidung für oder gegen eine Software als probates Gegenmittel für Datenschutzsorgen zuzulassen. Zugleich gewinnen Datenschutzsorgen durch die Gefahr von beruflichen Nachteilen oder sogar Jobverlust an Gewicht.

Die im Jahr 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) verankerte wegen solcher Risiken Werte

und Datenschutzprinzipien in der Gesetzgebung und definierte eindeutige Rechte für Individuen in Bezug auf ihre persönlichen Daten. Das Prinzip Privacy by Design findet sich hier zum Beispiel in Artikel 25 („Datenschutz durch Technikgestaltung und durch datenschutz-freundliche Voreinstellungen“) wieder. Dabei war ein wichtiges Ziel, die Datensouveränität zu stärken und den Betroffenen Kontrolle über die Verarbeitung ihrer Daten zu geben. Während dieser zusätzliche Schutz wichtig war und die Situation deutlich verbessert hat, reicht er doch nicht aus, um Missbrauch von Daten zu vermeiden. Zugleich kann die präventive Natur des Gesetzes legitime und sinnvolle Datennutzung einschränken. Verarbeitungsprozesse persönlicher Daten können nun die vorherige Einwilligung von Individuen erfordern, wenn keine anderen Rechtfertigungsgründe bestehen. In diesem Fall müssen Individuen zum Zeitpunkt der Einwilligung verstehen, was ihre Datenfreigabe bewirken wird. Das kann bereits bei legitimer Datennutzung schwer sein, vor allem wenn technisches Wissen über die Systeme fehlt, aber eine unvorhergesehene Nutzung oder ein Missbrauch von Daten sind nicht kontrollierbar. Das erzeugt Sorgen (siehe Teebken & Hess⁵), die ein risikovermeidendes Verhalten begünstigen. Wo es für Nutzerinnen und Nutzer also möglich ist, werden Datenfreigaben eingeschränkt und Dateneingaben minimiert. Auf der anderen Seite führt erzwungene oder betrieblich notwendige Transparenz aufgrund dieser Sorgen möglicherweise zu Reaktanz (siehe Feng et al.³), Unzufriedenheit mit dem Arbeitgeber oder psychischer Belastung (siehe Bhawe et al.¹).

Wir sehen das Problem in der fehlenden Einbeziehung der betroffenen Personen im Softwaredesign. Statt sich, wie bisher, nur auf die Nutzer der Software zu fokussieren, sollte Software bereits mit dem Gedanken an die Transparenzinteressen von Datensouveränen entwickelt werden, um Inverse Transparenz zu realisieren. Dafür schlagen wir einen neuen Ansatz vor: „Transparency by Design“.

46

2_ Ein neuer Weg für Software am Arbeitsplatz – Transparency by Design

Klassischerweise richten sich die Methoden des Software-Engineering auf die Nutzerinnen und Nutzer der Software aus. Mit seinem Buch „Usability Engineering“ (Software-Ergonomie) führte Jakob Nielsen 1993 (siehe Nielsen⁴) hier einen neuen Standard ein, dem die Idee zugrunde lag, die Nutzbarkeit von Software für ihre Anwender zu verbessern. Der Fokus lag erstmals nicht mehr rein auf der Funktionalität oder den

Kosten, sondern auf individuellen Faktoren in der Interaktion von Mensch und Software. Wie oben beschrieben glauben wir im Sinn des Design Thinking, dass als neue Interessenvertreter bei der Softwareentwicklung die Datensouveränen primär in den Blick genommen werden sollten.

Wie wir beschrieben haben, können die heute übliche fehlende Transparenz über die Datenverarbeitung sowie das

Ignorieren der Datenschutzsorgen von Mitarbeitenden zu Problemen im Betrieb führen. Führungskräfte sollten daher ein natürliches Interesse an einem verbesserten Umgang haben. Jedoch glauben wir, dass auch Softwarehersteller profitieren können. In vielen Betrieben in Deutschland ist es üblich, dass Mitarbeitende über die Mitbestimmung eine indirekte Einkaufsmacht ausüben können, was neue Software betrifft. Durch die Mitbestimmungspflicht zum Beispiel bei Einrichtungen zur Leistungs- und Verhaltenskontrolle sind solche Rechte auch gesetzlich verankert. Wenn ein Tool die Datenschutzsorgen nicht ausreichend adressiert, könnte die Konsequenz sein, dass es gar nicht gekauft wird oder ein Unternehmen sich zumindest nach Alternativen umsehen wird.

Dabei begegnet der Datenschutz so, wie er heute konzipiert ist, im Softwaredesign der Komplexität der entwickelten Tools nicht adäquat. Wir identifizieren diesbezüglich drei wichtige Treiber:

1. Anwendungsfälle werden komplexer und die Datennutzung schwerer überschaubar, vor allem für technisch nicht versierte Nutzerinnen und Nutzer.
2. Eine pauschale Entscheidung für oder gegen eine Datenfreigabe ist oft nicht sinnvoll treffbar, da viel vom Kontext der Nutzung abhängt.
3. Software entwickelt sich kontinuierlich weiter (agile Entwicklung, Software-as-a-service), weshalb Wissen über die Datenverarbeitung schnell veraltet.

Doch was ist die Alternative? Wir schlagen Transparency by Design vor (siehe Zieglmeier & Pretschner¹⁰). Grundprinzip ist eine Weiterentwicklung von Privacy by Design: Bereits bei der

Konzeption von Software sollte Datennutzungstransparenz mitgedacht werden, um Softwaredesign für empowerte Datensouveräne zu ermöglichen.

1.1_Das Konzept von Transparency by Design

Die grundlegende Idee von Transparency by Design basiert direkt auf dem Konzept der Inversen Transparenz: Wenn Datennutzende wie zum Beispiel Führungskräfte im Unternehmen auf Daten zugreifen (diese nutzen), sollen Datensouveräne gemäß dem Prinzip „Watch the Watcher“ darüber Transparenz erhalten. Konzeptuell erfordert das drei Schritte:

1. Überwachung aller Datenzugriffe
2. Verifizierung der Authentizität der Zugriffe und Speicherung
3. Verfügbarmachen der gespeicherten Zugriffe

Wir können diese drei Schritte, wie im Softwaredesign üblich, auf jeweils getrennte konzeptionelle Komponenten übertragen. Jede Komponente bekommt eine von den anderen Komponenten getrennte Aufgabe. Das ermöglicht uns bei der konkreten Umsetzung in die Praxis, die Implementierungen auszutauschen oder zu variieren, ohne das grundlegende Konzept zu verändern. Entsprechend ergeben sich aus dieser Liste drei konzeptuelle Komponenten: Ein *Monitor* überwacht Datenzugriffe [1], eine *Überwachungsinstanz* prüft und speichert das Nutzungsprotokoll [2] und das *Anzeigentool* macht die Information für den Datensouverän verfügbar [3]. Schematisch ist das in Abbildung 1 zu sehen.

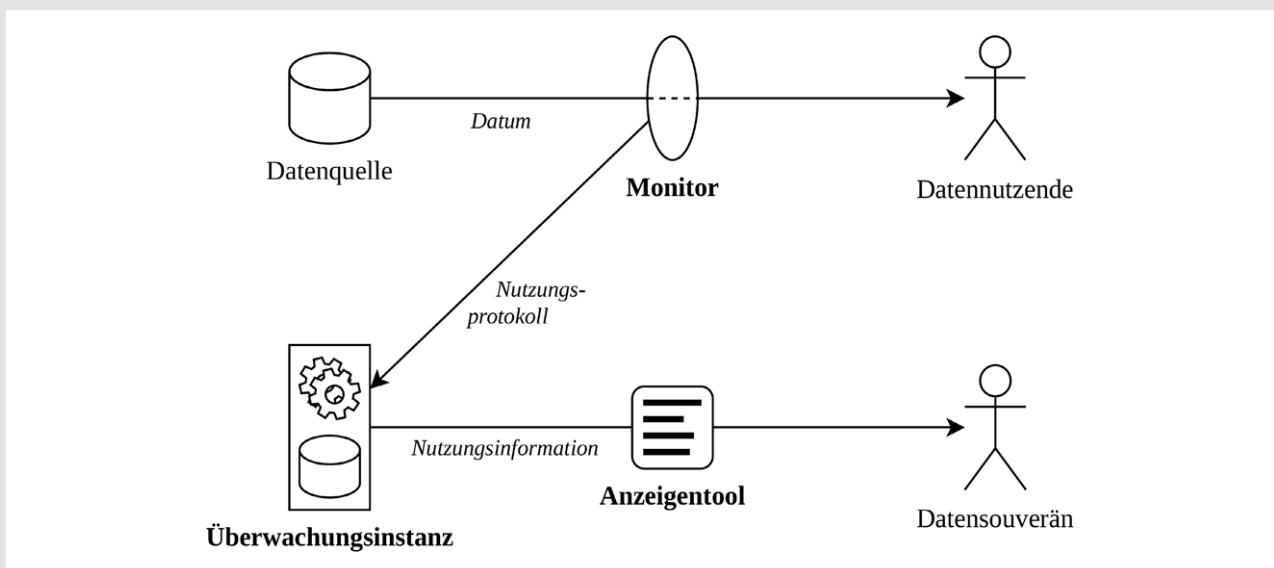


Abbildung 1: Transparentmachen von Datenzugriffen durch ein konzeptionelles Framework für Transparency by Design (Zieglmeier & Pretschner¹⁰)

1.2_ Implikationen für Softwaredesign

Nun stellt sich die Frage, wie sich das abstrakte Konzept auf konkretes Softwaredesign auswirkt. Daten werden üblicherweise nicht über kontrollierte Kanäle an Datennutzende „geschickt“, sondern bewegen sich ständig zwischen (Teil-) Systemen hin und her, werden aggregiert, kopiert, konvertiert oder verschoben. Ein „Zugriff“ könnte hier einfach bedeuten, dass ein datenbasiertes Tool gestartet wird – allein für die Anzeige normaler Startseiten werden Datenzugriffe nötig. Was ist also ein Datenzugriff und wie können wir sicherstellen, dass wir ihn protokollieren?

Um diese Frage zu beantworten, gehen wir zurück auf den Zusatz „by Design“ des Konzepts. Wir setzen beim Softwaredesign an, denn hier werden die Anwendungsfälle definiert und die Datenflüsse modelliert. Dabei erwartet Transparency by Design, dass bereits in der Konzeptphase einer Software, die mit persönlichen Daten arbeitet, die Transparenz für Datensouveräne über die Verarbeitung ihrer Daten mitgedacht wird. Solange dabei Daten nur im System verschoben oder manipuliert werden, ohne Datennutzenden zur Verfügung gestellt zu werden, besteht kein Änderungsbedarf. Dieser wichtige Aspekt ist auch der Grund, wieso die Transparenz nicht einfach im Nachhinein ermöglicht werden kann: Jegliche Überwachung einer existierenden Software läuft Gefahr, entweder relevante Zugriffe zu übersehen oder irrelevante Zugriffe unnötig zu protokollieren und dadurch Datensouveräne zu überfordern. Ein Nutzungsprotokoll soll genau ab dem Moment angelegt werden, in dem Datennutzende letztlich Zugriff auf die Daten erhalten.

Sofort ergeben sich Folgefragen. Viele Tools erlauben Exportfunktionen oder arbeiten direkt mit Dateien auf dem Speicher, die auch extern zugreifbar sind. Wie sollen diese Daten effektiv überwacht werden? Gar nicht. Denn während es heute noch gängig ist, Nutzern und Nutzerinnen Zugriff auf die unterliegenden Dateien zu geben, zum Beispiel über Exportfunktionen oder Netzwerkspeicher, ist ein klarer Trend hin zu Cloud-Software zu erkennen, die nur noch als „Service“ angeboten wird. Daten sind hier nicht mehr Dateien, über die die Nutzenden verfügen, sondern abstrakte Konzepte, die Funktionen ermöglichen. Dadurch verlieren Nutzer so viel Kontrolle, dass in Artikel 20 der DSGVO sogar bereits wieder

Datenportabilität und ein Recht auf Export gefordert wird. Auf den ersten Blick scheint dieses Recht sogar in Konflikt mit unserem Konzept zu stehen, aber hier lohnt ein genauerer Blick: Es bezieht sich ausschließlich auf die eigenen Daten, bei denen natürlich kein Risiko für Missbrauch besteht, wenn sie dem Datensouverän selbst zur Verfügung stehen.

Schwerer wiegt die Frage nach dem Umgang mit Daten-

Daten sind hier nicht mehr Dateien, über die die Nutzenden verfügen, sondern abstrakte Konzepte, die Funktionen ermöglichen.

zugriffen, die wir als „Umgebungsnutzung von Daten“ (ambient usage) bezeichnen wollen. Ein Beispiel soll zur Illustration helfen: Das Tool Jira Software von Atlassian, das die Planung und Verwaltung von Softwareprojekten ermöglicht, dient uns im Projekt als Anwendungsbeispiel. Wenn hier die Startseite geöffnet wird, was automatisch beim Aufruf des Tools passiert, öffnet sich ein sogenanntes „Dashboard“. Das ist nichts weiter als eine Ansammlung von kleinen Fenstern, die jeweils eine eigene Analyse, Funktion oder Sicht auf Daten darstellen (siehe Abbildung 2). In einem üblichen Dashboard, wie dem unten dargestellten, ist dabei meist nur ein Teil der Fenster zeitgleich sichtbar. Wenn eine Datennutzerin nun also Jira Software öffnet, um einfach eine Suche durchzuführen, wird sie trotzdem automatisch das Dashboard laden. Auch wenn sie dieses nicht beachtet und sofort auf die Suche wechselt, finden hier unzählige Datenzugriffe statt.

Wenn diese Zugriffe nun alle protokolliert werden, könnte das Datensouveräne verunsichern und verwirren. Zugleich wäre es wohl unmöglich, zu erkennen, ob die Datennutzerin die auf dem Dashboard sichtbaren Analysen vielleicht doch beachtet hat. Eye-Tracking mag theoretisch eine Lösung sein, praktisch wäre es wohl zu invasiv und nicht umsetzbar.

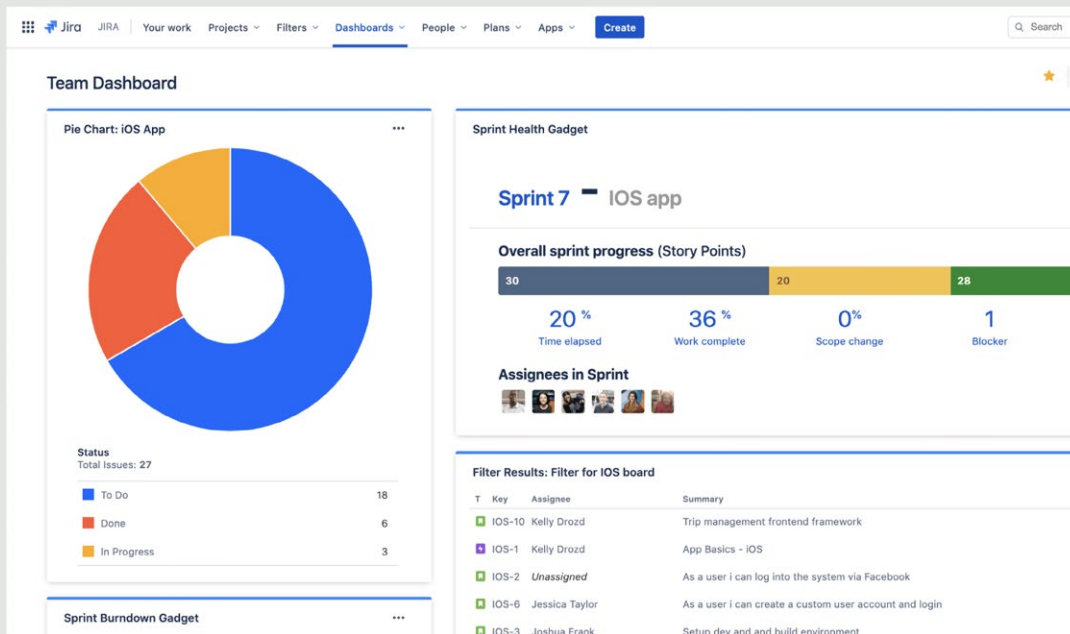


Abbildung 2: Ein beispielhaftes Dashboard von Jira Software (Quelle: www.atlassian.com)

Stattdessen könnte eine Konsequenz im Umgang mit solcher Umgebungsnutzung von Daten sein, dass sich Interaktionsparadigmen grundlegend verändern. Eine Möglichkeit wäre, dass nicht automatisch unzählige Datenzugriffe ge-

macht werden, ohne dass die Datennutzenden sich bewusst dafür entscheiden. Am Beispiel des Dashboards könnte das bedeuten, Analysen nur auf explizite Anfrage freizuschalten und sonst zu verbergen (siehe Abbildung 3).

49

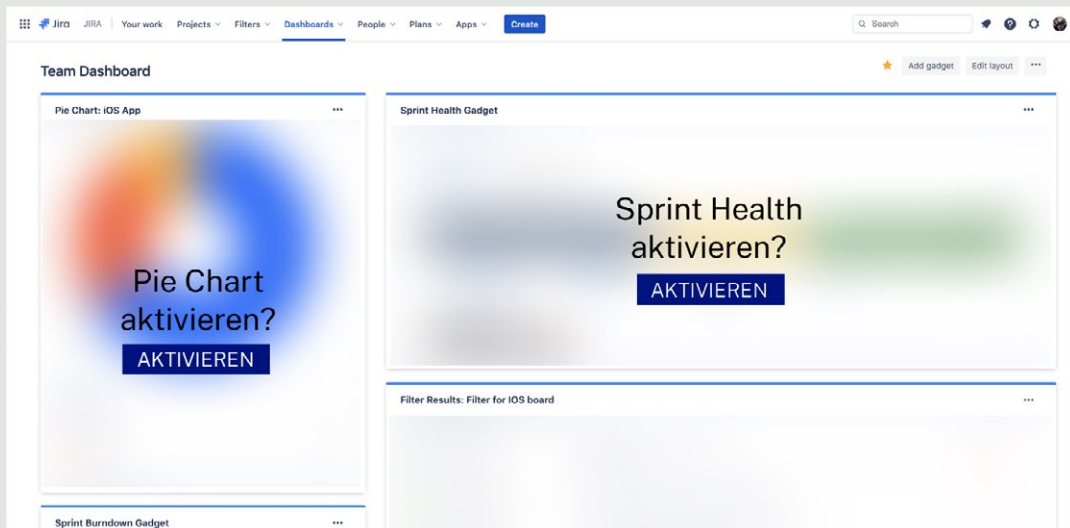


Abbildung 3: Modifiziertes Dashboard von Jira Software mit Transparency by Design (Anpassungen durch die Autoren)

Langfristig könnte sich durch Transparency by Design Software also weg von den aktuellen Prinzipien der freien Datennutzung und „Beliebigkeit“ von Analysen hin zu einem bewussteren Umgang mit Daten verändern.

1.3_ Fälschungssichere und vollständige Protokollierung

Bis hierhin haben wir uns mit der Überwachung von Datenzugriffen befasst. Tendenziell liegt in diesem Schritt auch die wichtigste Grundlage für Inverse Transparenz; doch ohne fälschungssicheres Protokoll (Überwachungsinstanz, siehe Abbildung 1) entfaltet sie nicht ihr volles Potenzial.

Dabei steht die Vertrauenswürdigkeit der gesammelten Protokolle im Fokus. Vertrauen in die Nutzungsprotokolle ist eine zentrale Voraussetzung, um das Potenzial von Inverser Transparenz zu realisieren. Es wird schnell klar, dass ein unvollständiges oder manipuliertes Protokoll keinen Wert darstellt. Wenn Mitarbeitende sich nicht auf eine korrekte und fälschungssichere Protokollierung verlassen können, verlieren die Daten ihre Macht. Wir müssen dabei vor allem für die Integrität der Daten garantieren. Das bedeutet: Wir benötigen die Sicherheit, dass jede Datennutzung in einem Protokolleintrag gespeichert wird, aber genauso wichtig ist, dass jedem Eintrag wiederum eine tatsächlich stattgefundene Datennutzung zugrunde liegt.

Hierbei können wir verschiedene Ansätze identifizieren, die diese Integrität sicherstellen können. Dabei lohnt es sich, aus der Perspektive der Nutzer von Inverser Transparenz, also der Datensouveräne und Datennutzenden, zu denken. Beide haben ein Interesse daran, dass die Nutzungsprotokolle

vollständig und korrekt sind. Datensouveräne, weil sie die Sicherheit wollen, dass kein Datenmissbrauch unerkannt bleibt. Datennutzende, weil sie nicht aufgrund von manipulierten Nutzungsdaten in Schwierigkeiten geraten wollen. Für unsere Überlegungen im Folgenden ist es dabei nicht relevant, ob die Überwachungsinstanz, beziehungsweise ihre Funktion, als separates Programm oder als Teil der Software selbst realisiert wird; konzeptionell ändert sich nichts.

Wir müssen davon ausgehen, dass jede Mitarbeiterin und jeder Mitarbeiter im Unternehmen sowohl als Datensouverän als auch als Datennutzer und –nutzerin agieren kann, inklusive der höchsten Entscheiderinnen und der Systemadministration. Das bedeutet, dass potenziell jede Partei ein Manipulationsinteresse haben kann. Insofern gehen wir von einer „Umgebung ohne Vertrauen“ (trust-free environment) aus. In den letzten Jahren entwickelt sich eine Sicherheitstechnologie von Intel, die sogenannten Software Guard Extensions (SGX), zur logischen Wahl für solche Umgebungen. Ohne zu tief ins Detail zu gehen, wird hier durch kryptographische Methoden und eine abgeschottete Umgebung im Computerprozessor sichergestellt, dass Programme und Daten auch auf nicht kontrollierbaren Systemen manipulationsfrei bleiben. Die Technologie hat Potenzial und kann in unserem Fall als Lösung dienen, doch erfordert sie weiterhin Vertrauen – vor allem in Intel als Hersteller des Prozessors.

Deshalb haben wir auch alternative Wege erforscht, mit dem Ziel, in einer Umgebung ohne Vertrauen komplett auf Basis kryptographischer Methoden die Integrität der Nutzungsprotokolle sicherzustellen: mit Blockchain-Technologie (siehe Zieglmeier & Loyola Daiqui⁹). Zugrunde liegt hierbei die Idee, dass alle, die am System teilnehmen, eine Kopie der Nutzungsprotokolle in verschlüsselter Form als Blockchain speichern. Bei einer Zugriffsanfrage wird kein Zentralrechner angefragt, sondern ein sogenannter Knoten, der dem Datensouverän gehört, bekommt die Anfrage zugestellt. Wenn der Zugriff zugelassen wird, erstellt dieser Knoten automatisiert einen Protokolleintrag und verteilt diesen im Netzwerk.

50

Langfristig könnte sich durch Transparency by Design Software also weg von den aktuellen Prinzipien der freien Datennutzung und „Beliebigkeit“ von Analysen hin zu einem bewussteren Umgang mit Daten verändern.

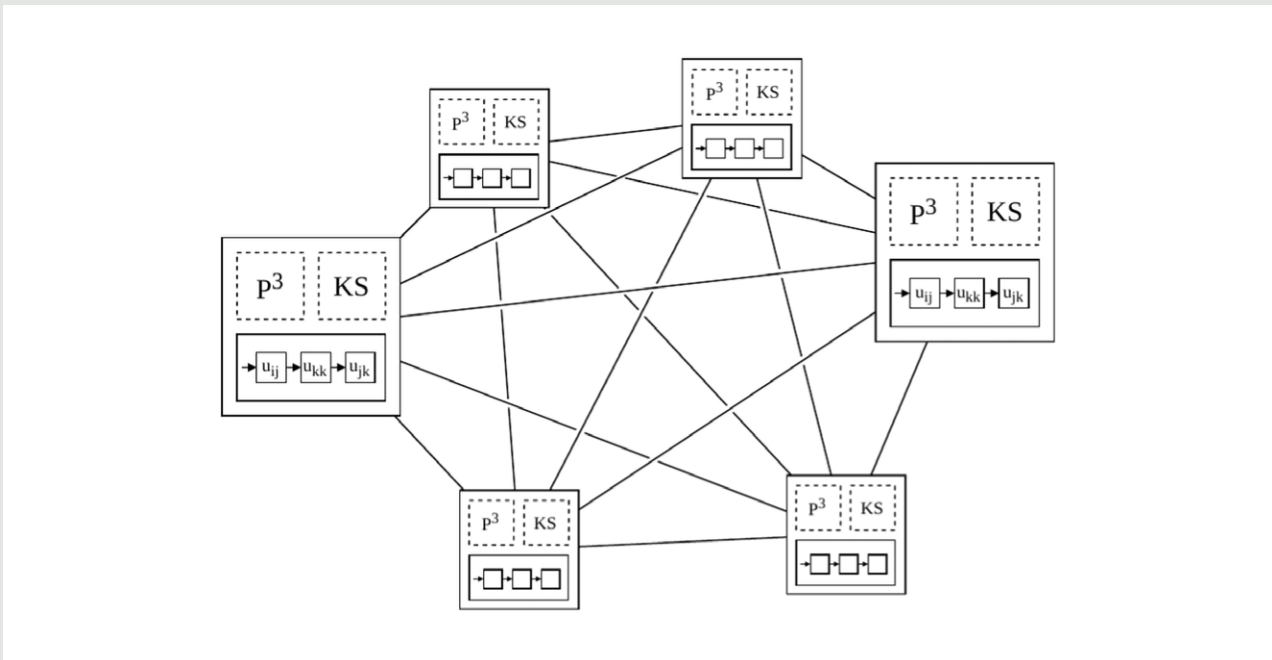


Abbildung 4: Peer-to-peer-Architektur des Blockchain-Netzwerks (Zieglmeier & Loyola Daiqui⁹)

Blockchainlösungen sind oft in der Kritik, vor allem wegen der hohen Energieverbräuche, aber auch wegen der Frage nach ihrer Notwendigkeit. In unserem Konzept stellt zumindest ersteres kein Problem dar: Statt auf die üblichen energieintensiven Mechanismen zur Verifizierung zu setzen, können wir mithilfe der echten Identitäten der Netzwerkteilnehmenden und des Proof-of-Authority-Prinzips (siehe Wood⁸) ähnliche Garantien geben, ohne große Energieverbräuche zu erfordern. Auf der anderen Seite ist aber die Frage nach der Notwendigkeit einer Blockchain weniger eindeutig zu beantworten.

Idealerweise handelt es sich am Arbeitsplatz nicht um eine Umgebung ohne Vertrauen, weshalb eine Technologie wie Blockchain vielleicht nicht notwendig ist. Allerdings stellt sich die Frage, in welchen Fällen das nicht mehr zutrifft und ob nicht gerade dann den Nutzungsprotokollen besonderer Wert zukommt. Speziell der Fall eines Streits mit einer Führungskraft scheint hier relevant zu sein. Nehmen wir an, dass ein Missbrauch von Daten durch die Führungskraft erfolgt ist, um eine unerlaubte Leistungskontrolle durchzuführen. Nach diesen

Analysen wird dem Mitarbeiter gekündigt, weshalb er sich zur Wehr setzen will. Er prüft das Protokoll der Datenzugriffe, um mögliches Fehlverhalten zu erkennen. Kann er in dieser Situation noch auf die Systeme der Firma vertrauen? Die Führungs-

51

Es liegt nahe, dass nur eine Lösung komplett ohne Notwendigkeit von Vertrauen hier verlässlich als Datengrundlage dienen kann.

kraft könnte gut vernetzt sein und hat möglicherweise bereits die Anweisung zum Löschen der belastenden Daten gegeben. Es liegt nahe, dass nur eine Lösung komplett ohne Notwendigkeit von Vertrauen hier verlässlich als Datengrundlage dienen kann. Trotzdem wird es wichtig bleiben, als Maxime nicht absolute Sicherheit anzustreben, sondern auch die Nutzbarkeit im Auge zu behalten (siehe dazu auch Tøndel et al.⁶).

3_ Die technische Umsetzung Inverser Transparenz in der Praxis – das Konzept der Toolchain

Im Rahmen des Forschungsprojekts haben wir uns zum Ziel gesetzt, die Idee der Inversen Transparenz in die Praxis zu bringen und im Rahmen eines betrieblichen Praxislaboratoriums bei der Software AG zu erproben. Von zentraler Bedeutung für dieses Vorhaben war, die abstrakten Ideen auf konkrete und adressierbare Probleme zu reduzieren. Im ersten Schritt identifizierten wir deshalb einen relevanten Anwendungsfall bei unserem Praxispartner Software AG: das Tool Jira Software. Nun sollte es im zweiten Schritt darum gehen, die theoretisch konzeptionierte Transparenzlösung (siehe Abbildung 1) in die

Praxis zu bringen. Da wir mit einer vorhandenen Software-Suite umgingen, entwickelten wir in einem mehrschrittigen Verfahren eine realisierbare Umsetzung der Inversen Transparenz in der Praxis: die Inverse-Transparenz-Toolchain.

Den Prinzipien „Trennung der Belange“ (separation of concerns) und Software-as-a-service folgend, realisierten wir jede konzeptionelle Komponente als selbstständigen Web-Service. Dabei erfüllt der „Overseer“ die Aufgabe der Überwachungsinstanz und die Web-App „Watch the Watcher“ ist das Anzeigentool (siehe Abbildung 5).

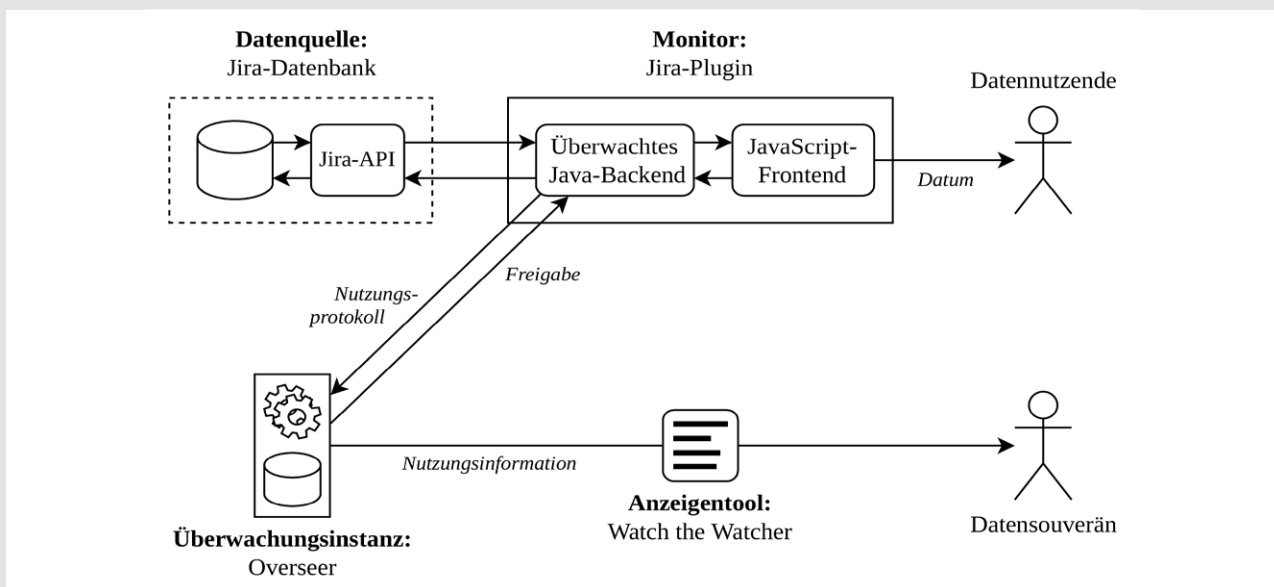


Abbildung 5: Instantiierung des Konzepts für Transparency by Design mit Web-Services am Anwendungsbeispiel Jira Software (Zieglmeier & Pretschner¹⁰)

Für den Monitor mussten wir eine Lösung finden, um Transparenz im laufenden Betrieb möglichst wenig invasiv und ohne tiefgehende Administrationsrechte auf dem Zielsystem zu realisieren. Unsere Lösung war deshalb die Entwicklung von vollintegrierten Plugins. Anhand von Abbildung 5 lässt sich unsere Umsetzung leicht erklären: Wir entwickelten Plugins, die Monitor-Funktionalität bereits in einem überwachten Java-Backend integrieren. Jede Anfrage an das

JavaScript-Frontend (die Fenster des Dashboards, siehe auch Abbildung 2) löst dann automatisch eine Protokollierung in der Überwachungsinstanz „Overseer“ aus.

Nun ist es spannend zu beobachten, welche Anwendungsfälle sich auf Basis der Toolchain realisieren lassen und welche Weiterentwicklungen und Anpassungen an den Tools sich aus dem Einsatz in der betrieblichen Praxis ergeben.

4_ Zusammenfassung

Wir argumentieren, dass Softwaredesign sich weiterentwickeln muss. Als nächsten Schritt nach Privacy by Design, einer wichtigen Grundlage für den Datenschutz, schlagen wir deshalb Transparency by Design vor: das Mitdenken der Transparenzinteressen der Datensouveräne bereits bei der Entwicklung, um Inverse Transparenz zu realisieren. Das bedeutet einen Wandel vom stark präventiven Umgang mit Daten (Privacy by Design) hin zu mehr Offenheit, flankiert durch vollständige Transparenz über die Verarbeitungsprozesse (Transparency by Design). Drei Treiber begründen dies hauptsächlich: Komplexere Anwendungsfälle erschweren die Überschaubarkeit von Systemen [1], pauschale Entscheidungen für oder gegen Datenfreigaben sind ohne Kontext nicht treffbar [2] und Software ist nicht mehr statisch, sondern

entwickelt sich laufend weiter, was regelmäßige Überprüfbarkeit erforderlich macht [3]. Dabei glauben wir, dass diese Veränderung im Softwaredesign fundamentale Änderungen an Interaktionsparadigmen zur Folge haben kann und das Potenzial hat, die Datensouveränität von Individuen zu stärken. Um das Konzept der Inversen Transparenz unmittelbar erlebbar zu machen und unsere Hypothesen auf den Prüfstand stellen zu können, haben wir deshalb eine konkrete Umsetzung von Inverser Transparenz in Form der Toolchain entwickelt, die uns im Praxislaboratorium als technische Grundlage diene. Im Zusammenspiel zwischen Toolchain und Praxislaboratorium liegt ein zentraler Wert unseres Forschungsansatzes.

5_ Referenzen

- 1 Bhave, Devasheesh P., Teo, L., Dalai, R. Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management*, 46, 1 (2020), 127–164. Supplementals.
- 2 Cavoukian, A. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, 2009.
- 3 Feng, W., Tu, R., Lu, T., Zhou, Z. Understanding forced adoption of self-service technology: The impacts of users psychological reactance. *Behaviour & Information Technology*, 38, 8 (2019), 820–832.
- 4 Nielsen, J. Usability Engineering. Academic Press, 1993.
- 5 Teebken, M., Hess, T. Privacy in a Digitized Workplace: Towards an Understanding of Employee Privacy Concerns. In Proceedings of the 54th Hawaii International Conference on System Sciences. 2021, 6661–6670.
- 6 Tøndel, I. A., Soares Cruzes, D., Jaatun, M. G. Achieving 'Good Enough' Software Security: The Role of Objectivity. In Proceedings of the Evaluation and Assessment in Software Engineering. April 2020, 360–365.
- 7 Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G. J. Information Accountability. Computer Science and Artificial Intelligence Laboratory Technical Report, MIT-CSAIL-TR-2007-034. June 2007.
- 8 Wood, G. Proof-of-authority private chains. 2015. <https://github.com/ethereum/guide/blob/master/poa.md>.
- 9 Zieglmeier, V., Loyola Daiqui, G. (2021). GDPR-Compliant Use of Block-chain for Secure Usage Logs. In Proceedings of the Evaluation and Assessment in Software Engineering. June 2021, 313–320.
- 10 Zieglmeier, V., Pretschner, A. Trustworthy transparency by design. Vorveröffentlichung auf arXiv (2021). arXiv:2103.10769.

Verbundkoordination:
Prof. Dr. Andreas Boes, PD Dr. Tobias Kämpf
Institut für Sozialwissenschaftliche Forschung e.V.
Jakob-Klar-Str. 9
80796 München
www.inversetransparenz.de
© 2022 ISF München

ISFMÜNCHEN

Empfohlene Zitierweise:
Andreas Boes, Thomas Hess, Alexander Pretschner,
Tobias Kämpf, Elisabeth Vogl (Hrsg.) (2022):
Daten – Innovation – Privatheit – Mit Inverser
Transparenz das Gestaltungsdilemma der digitalen
Arbeitswelt lösen. München.
https://doi.org/10.36194/INVERSETRANSPARENZ_Mai_2022

Konzept & Redaktion: Elisabeth Vogl, Dr. Jutta Witte
Lektorat: Frank Seiß, ISF München
Gestaltung: Jochen Härtel, designteam.eu

Gefördert von



Bundesministerium
für Bildung
und Forschung