CDPS
TUM CENTER FOR DIGITAL PUBLIC SERVICES

Rechtliche Stellungnahme im Rahmen des Projekts Inverse Transparenz

16.05.2022

Prof. Dr. Dirk Heckmann

Ass. Jur. Pascal Bronner

Ass. Jur. Valentin Vogel

f

A. Grundlagen

I. Einführung in das Projekt

Die durch die zunehmende Automatisierung und Vernetzung von Systemen, Prozessen und Daten geprägte **digitale Transformation** bewirkt einen umfassenden gesellschaftlichen Wandel in praktisch allen Lebensbereichen, vor allem auch im **Beschäftigungskontext**.[1] Neben der nicht mehr wegzudenkenden Nutzung von IT-Systemen, umfasst die Digitalisierung am Arbeitsplatz insbesondere die Einkehr eines vielfältigen und unstreitig nützlichen Angebots an **Tools und Software**, die zur Unterstützung von Arbeitsabläufen und -ergebnissen genutzt werden.[2] Die Nutzung und Vernetzung diverser Softwareangebote führt wiederum zu einem enormen Anfall an Datenbeständen, der erhebliche **Chancen**, aber auch **Risiken** mit sich bringen kann. Gerade im Hinblick auf die steigenden Möglichkeiten der Arbeitgeberinnen und Arbeitgeber, Daten mit Softwaretools zu erheben, zu aggregieren und zu analysieren, können Bedenken und Verunsicherungen bei den Arbeitnehmerinnen und Arbeitnehmern entstehen. Denn durch die **komplexen Datenverarbeitungsmechanismen** moderner Softwaretools und die technische Entwicklung von Big Data oder KI-Anwendungen sind Art und Umfang der im Arbeitsalltag erhobenen Daten nicht mehr vollumfänglich einzuschätzen.[3] 1

So kann aufgrund der – u.a. technisch bedingten – fehlenden **Transparenz** **Verunsicherung** und Angst vor **Missbrauch**, ungerechtfertigten Leistungskontrollen sowie gläsernen Strukturen entstehen. Dies führt dazu, dass viele anfallende und gewinnbringende Daten nicht genutzt werden, sodass zwar die entstehenden Risiken hinreichend berücksichtigt, gleichwohl aber die damit einhergehenden Chancen verpasst werden. Durch das Konzept der Inversen Transparenz und der Entwicklung der **Inversen Transparenz Toolchain** soll an dieser Inkongruenz angesetzt werden. Dabei geht es darum, wirtschaftliche Interessen und die Schutzinteressen von Beschäftigten (mit Blick auf ihre personenbezogenen Daten und informationelle Selbstbestimmung) in Einklang zu bringen. Das **Konzept der Inversen Transparenz** soll einerseits datenbasierte Wertschöpfung und Innovation gewährleisten und andererseits die Kontroll- und Schutzmöglichkeiten der Beschäftigten in einer digitalen Arbeitswelt stärken, die durch asymmetrische Machtbeziehungen gekennzeichnet ist. Während in klassischen 2

---

[1] Laut einer Studie des Bundesministeriums für Arbeit und Soziales (BMAS) nutzen durchschnittlich 83% der Beschäftigten IT-Systeme am Arbeitsplatz, s. BMAS Monitor: Digitalisierung am Arbeitsplatz, S. 6, https://www.bmas.de/DE/Service/Publikationen/a875-monitor-digitalisierung-am-arbeitsplatz.html.

[2] Beispielhaft genannt sei hier Software zur Mailverarbeitung, Textverarbeitung, Kalkulation und Präsentation (z.B. Microsoft Office), zur Kommunikation (z.B. Slack), der insbesondere seit der Covid19-Pandemie nicht mehr verzichtbaren (Video-)Telefonie (z.B. Zoom, Skype), zur Fehlerverwaltung und Problembehandlung (z.B. *Jira*), zum Projektmanagement (z.B. Trello, Asana) oder zur Personalverwaltung (z.B. Personio) bzw. zur Verwaltung von Reisekosten und Auslagen (z.B. Circula).

[3] Zur schweren Bestimmbarkeit der Datenerhebungen vgl. *Kämpf/Vogl/Boes*, Forschungsreport Inverse Transparenz, S. 25.

Arbeitsstrukturen Transparenz nur einseitig gegeben ist, indem Führungskräfte und Arbeitgeberinnen und Arbeitgeber exklusiv Daten über Mitarbeitende (als passive Informationssubjekte) haben[4], werden die Mitarbeitenden im Rahmen der Inversen Transparenz **aktiv** in die Gestaltung und Nutzung der Daten **einbezogen**.[5] Inverse Transparenz bietet theoretisch das Potenzial, Datenverwendungen nachzuvollziehen sowie Datenmissbrauch zu erkennen und zu problematisieren - bzw. bei Ausbleiben von Missbrauch Vertrauen in die konforme Nutzung von Daten zu gewinnen. Die Nutzung der Daten zwischen Vorgesetzten und Mitarbeitenden sowie unter Mitarbeitenden können im Konzept wechselseitig transparent gemacht werden. Dadurch können Mitarbeiter und Mitarbeiterinnen z.B. die Datenzugriffe von Vorgesetzten einsehen (Prinzip „**Watch the Watcher**"), sodass die Verunsicherung über mögliche Missbrauchspotentiale sinkt und das Vertrauen in die Datennutzung steigt.[6] Durch die Auflösung der einseitigen Transparenzstruktur und die aktive Einbindung der Mitarbeitenden soll ihr **Empowerment** zur gleichberechtigten und innovativen Datennutzung gestärkt und innovative Führungskonzepte ohne einseitige Informationsherrschaft ermöglicht werden.[7] Inverse Transparenz ist dabei ein innovatives Konzept, das das Potenzial hat, die datenschutzrechtlichen Grundsätze Privacy by Design und Privacy by Default zu ergänzen. Da diese Konzepte mit der Digitalisierung an ihre Grenzen geraten, sollte im Projekt exploriert werden, wie Inverse Transparenz durch die Erweiterung der Kontrollmöglichkeiten der Datensubjekte einen effektiven Schutz von Beschäftigtendaten ermöglichen kann.

3 Für die rechtliche Begutachtung des Projekts sollen in einem ersten Schritt die aktuellen **Grundsätze des Datenschutzes** sowie des **Arbeitnehmerdatenschutzes** mit Bezügen zum Recht der **Leistungskontrolle** dargestellt werden. In einem zweiten Schritt erfolgt die technische und rechtliche Einordnung der im Projekt entwickelten praktischen Umsetzung des Konzepts durch die Inverse Transparenz Toolchain im aktuellen gesetzlichen Rahmen (de lege lata). So können mögliche Probleme erkannt und Handlungsempfehlungen für die Zukunft identifiziert werden (de lege ferenda).

---

[4] *Kämpf/Vogl/Boes*, Forschungsreport Inverse Transparenz, S. 30.
[5] *Kämpf/Vogl/Boes*, Forschungsreport Inverse Transparenz, S. 30 f.
[6] *Kämpf/Vogl/Boes*, Forschungsreport Inverse Transparenz, S. 30 f.; *Hess/Neuburger/Gierlich-Joas*, Forschungsreport Inverse Transparenz, S. 39.
[7] *Kämpf/Vogl/Boes*, Forschungsreport Inverse Transparenz, S. 31.

II. Grundlagen Datenschutzrecht

1. Recht auf Informationelle Selbstbestimmung

Das (Grund-)**Recht auf informationelle Selbstbestimmung** ist in Deutschland bereits seit dem wegweisenden Volkszählungsurteil[8] des BVerfG 1983 als Ausprägung des Allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i. V.m. Art. 1 Abs. 1 GG anerkannt. Dies umfasst das Recht des Einzelnen, grundsätzlich. selbst über die Verwendung und Preisgabe seiner personenbezogenen Daten zu bestimmen. Schon im damaligen Urteil stellte das BVerfG fest, dass es keine belanglosen Daten mehr gebe[9], die Erhebung minimiert werden und ein Schutz vor unbegrenzter Datenverarbeitung durch die Schaffung der informationellen Selbstbestimmung erfolgen müsse.[10] 4

2. Verhältnis DSGVO und nationale Bestimmungen

Die rechtlichen Grundlagen des Datenschutzes orientieren sich in Deutschland aktuell primär an der unionsrechtlichen Datenschutzgrundverordnung (**DSGVO**). Diese gilt als Verordnung der EU (Art. 288 Abs. 2 AEUV) in den Mitgliedsstaaten **unmittelbar** und legt einen umfassenden Rahmen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für öffentliche sowie nichtöffentliche Stellen fest.[11] An einigen Stellen eröffnet die DSGVO für die Mitgliedsstaaten in sog. **Öffnungs- bzw. Spezifizierungsklauseln** die Möglichkeit, Teilbereiche des Datenschutzrechts in nationalen Bestimmungen gesondert zu regeln, zu spezifizieren oder innerhalb eines vorgegebenen Rahmens festzulegen.[12] Die Umsetzung dieser Klauseln ist in Deutschland neben bereichsspezifischen Regelungen (z.B. Sozialdatenschutz im SGB X[13]/I) in den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) und der Landesdatenschutzgesetze umgesetzt worden. Daneben werden dort Teilbereiche geregelt, die vom Anwendungsbereich der DSGVO nicht erfasst sind (z.B. Die Umsetzung der Datenschutzrichtlinie für Polizei und Justiz) oder die Ausgestaltung von Pflichten betreffen.[14] Soweit im Rahmen der Öffnungsklauseln nicht abschließend alles geregelt wurde, gelten die Regelungen der DSGVO weiter unmittelbar.[15] Innerhalb der nationalen Bestimmungen gehen nach § 1 Abs. 2 BDSG zunächst bereichsspezifische Regelungen den Regelungen des BDSG als lex specialis vor, soweit dort spezifische Regelungen zum 5

---

[8] BVerfGE 65, 1 = NJW 1984, 419.
[9] BVerfGE 65, 1 Rn. 152.
[10] BVerfGE 65, 1 Rn. 147 ff.
[11] Vgl. *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 70 ff.
[12] *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 73.
[13] Dazu *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 81f; Öffnungsklauseln finden sich für den Sozialdatenschutz z.B. in Art. 6 Abs. 2,3 oder Art. 9 Abs. 2 DSGVO, vgl. dazu *Greiner* in Knickrehm/Kreikebohm/Waltermann, Kommentar zum Sozialrecht, 7. Aufl. 2021, SGB I § 35 Rn. 2.
[14] Vgl. *Gola/Reif* in Gola/Heckmann, BDSG § 1 Rn. 22.
[15] Vgl. *Selmayr/ Ehmann* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Einführung Rn. 88.

Datenschutz getroffen werden.[16] Das BDSG dient in diesen Fällen dann insoweit als Auffanggesetz.[17]

3. Anwendbarkeit der DSGVO – Personenbezogene Daten und Sachdaten

6 Ob die DSGVO anwendbar und die Regelungen maßgeblich sind, bestimmt sich anhand eines **sachlichen** und **räumlichen Anwendungsbereichs**[18], wobei hier besonders auf den sachlichen Anwendungsbereich einzugehen ist. Der sachliche Anwendungsbereich ist gem. Art. 2 Abs. 1 DSGVO für die ganz oder teilweise automatisierte sowie nichtautomatisierte Verarbeitung[19] personenbezogener Daten eröffnet. **Personenbezogene Daten** sind nach Art. 4 Nr.1 DSGVO Informationen, die sich auf eine **identifizierte** oder **identifizierbare** natürliche Person beziehen. Der Personenbezug ist abzugrenzen von reinen Sachdaten, die keinen Bezug mehr zu einer Person erkennen lassen (z.B. Produktionsdaten).[20] Eine Person ist identifiziert, wenn die Informationen direkt auf die Person schließen lassen[21], sie ist identifizierbar, wenn sie mittels Zuordnung anderer Daten (z.B. Standortdaten, Online-Kennung) identifiziert, also „ermittelt"[22] werden kann.[23] Für die Feststellung der Identifizierbarkeit werden alle Mittel berücksichtigt, die im Rahmen der Ermittlung wahrscheinlich genutzt werden, um eine Identifizierung zu gewährleisten.[24]

4. Grundsätze des Datenschutzes

a) Verbotsprinzip mit Erlaubnisvorbehalt

7 Die datenschutzrechtlichen Regelungen nach DSGVO und BDSG unterliegen übergreifenden systematischen Grundsätzen, die aus den deutschen und europäischen Grundrechten hergeleitet werden können. Zentraler Grundsatz der DSGVO ist das **Verbot mit Erlaubnisvorbehalt**[25], der sich aus Art. 6 Abs. 1 DSGVO ergibt. Danach ist die Verarbeitung personenbezogener Daten grundsätzlich verboten, solange nicht die in Art. 6 DSGVO normierten Ausnahmetatbestände die Verarbeitung zulassen[26], sodass jede Datenverarbeitung mindestens eine der dort abgebildeten Rechtsgrundlagen erfordert[27], wenngleich auch mehrere gleichzeitig erfüllt sein können.

---

[16] *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 77ff.
[17] *Gola/Reif* in Gola/Heckmann, BDSG, 13. Aufl. 2019, § 1 Rn. 11.
[18] *Kühling/Raab* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 2 Rn. 1.
[19] Nach Art. 2 Abs. 1 DSGVO sind auch nichtautomatisierte Verarbeitungen maßgeblich, wenn sie in Dateisystemen gespeichert sind oder gespeichert werden sollen.
[20] *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 117.
[21] *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 120 mwN.
[22] *Gola* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 4 Rn. 5.
[23] Vgl. Art. 4 Nr. 1 Hs. 2 DSGVO.
[24] Vgl. Erwägungsgrund 26 S. 3 der DSGVO.
[25] Dazu *Buchner/Petri* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO Art. 6 Rn. 11ff.
[26] Vgl. dazu *Reimer* in Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, DSGVO Art. 6 Rn. 1.
[27] *Wolff* in Wolff/Brink, BeckOK Datenschutzrecht, 39. Edition, Syst. A Rn. 18.

Daher hat die privatautonome **Einwilligung** nach Art. 6 Abs. 1 lit. a) DSGVO eine zentrale Rolle inne, da sie auch zusätzlich zu gesetzlichen Tatbeständen eingeholt werden kann[28] und Sicherheit bieten kann. Weitere relevante und später differenziert zu prüfende Erlaubnistatbestände sind die erforderliche **Verarbeitung zur Erfüllung eines Vertrages** bzw. zur Durchführung vorvertraglicher Maßnahmen nach Art. 6 Abs. 1 lit. b) DSGVO, die Verarbeitung zur Erfüllung einer **rechtlichen Verpflichtung**[29] nach Art. 6 Abs. 1 lit. c) DSGVO sowie die Verarbeitung zur **Wahrung berechtigter Interessen** in einer Interessensabwägung nach Art. 6 Abs. 1 lit. f) DSGVO. 8

b) Grundsätze für die Verarbeitung personenbezogener Daten

Neben dem Verbotsprinzip mit Erlaubnisvorbehalt finden sich wesentliche – bußgeldbewehrte[30] - **Grundsätze** für die **Verarbeitung personenbezogener Daten** in Art. 5 DSGVO.[31] Die im Hinblick auf das Projekt relevantesten Grundsätze sollen im Folgenden kurz erläutert werden. 9

(aa) Grundsatz der Rechtmäßigkeit, Transparenz sowie von Treu und Glauben

Teilweise als ein Bestandteil des Grundsatz des verantwortungsvollen Datenumgangs zusammengefasst[32] normiert Art. 5 Abs. 1 lit. a) DSGVO, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Darin enthalten sind die drei Grundsätze der Rechtmäßigkeit, von Treu und Glauben sowie der Grundsatz der Transparenz. Nach dem **Grundsatz der Rechtmäßigkeit** sind Datenverarbeitungen nur rechtmäßig, wenn sie aufgrund einer Rechtsgrundlage, also durch gesetzliche Ermächtigung oder Einwilligung, erfolgen.[33] Der **Grundsatz der Verarbeitung nach Treu und Glauben** soll eine faire Datenverarbeitung gewährleisten[34] und ist aufgrund seiner Unbestimmtheit als Auffanggrundsatz zu verstehen.[35] Nach **dem Grundsatz der Transparenz** sollen die Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden, um das Recht auf informationelle Selbstbestimmung selbstbestimmt wahrnehmen zu können 10

---

[28] Vgl. dazu *Buchner/Petri* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 6 Rn. 22, zur Problematik der Suggestion der Entscheidungsmacht bei doppelter Einholung Rn. 23; zum Begriff vgl. Art. 4 Nr. 11 DSGVO.

[29] Die rechtliche Verpflichtung bezieht sich hierbei nicht auf vertragliche Pflichten, sondern gesetzliche Verpflichtungen, z.B. Aufzeichnungs- oder Dokumentations- oder Compliance-Pflichten, vgl. *Schulz* in Gola, DSGVO, 2. Aufl. 2018, Art. 6 Rn. 43.

[30] Vgl. Art. 83 Abs. 5 Buchst. a) DSGVO.

[31] Dazu *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 207ff.

[32] *Wolff* in Wolff/Brink, BeckOK Datenschutzrecht, 39. Edition, Syst. A Rn. 64ff, wobei danach auch weitere Grundsätze unter diesen dargestellten (Über)Grundsatz zu fassen sind.

[33] Vgl. dazu bereits zum Verbotsprinzip mit Erlaubnisvorbehalt; so *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 209.

[34] Vgl. dazu mwN *Voigt* in Taeger/Gabel, DSGVO-BDSG-TTDSG, DSGVO Art. 5 Rn. 13.

[35] So *Herbst* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO Art. 5 Rn. 17 mwN; zust. *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 225 mwN.

und potentielle Gefahren überhaupt erkennen zu können.[36] Konkretisierungen des Grundsatzes finden sich z.B. in den Betroffenenrechten nach den Art. 12ff. DSGVO (z.B. Auskunftsrecht).[37]

(bb) Grundsatz der Datenminimierung

11 Nach dem **Grundsatz der Datenminimierung** gem. Art. 5 Abs. 1 lit. c) DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Die Daten müssen zur Zweckerreichung erheblich, erforderlich[38] und angemessen sein, also in einem angemessenen Verhältnis zum jeweiligen Zweck stehen und geeignet sein, diesen zu erreichen.[39] Es dürfen also nur „so viele Daten wie nötig, aber gleichzeitig nur so wenig wie möglich gesammelt und verwendet werden".[40]

(cc) Grundsatz der Zweckbindung

12 Nach dem **Zweckbindungsgrundsatz** gem. Art. 5 Abs. 1 lit. b) DSGVO dürfen Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht mit einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Der Verantwortliche muss daher schon vor der Datenverarbeitung einen hinreichend festgelegten Zweck der Datenverarbeitung definieren[41] und darüber informieren. So wird sichergestellt, dass eine weiterführende und mehrfache Verarbeitung einmal erhobener Daten zu anderen Zwecken dem Grundsatz nach verhindert wird.[42]

(dd) Grundsatz der Vertraulichkeit und Integrität

13 Ein weiterer relevanter Grundsatz zum verantwortungsvollen Umgang mit Daten[43] findet sich im **Grundsatz der der Integrität und Vertraulichkeit** nach Art. Art. 5 Abs. 1 lit. f) DSGVO, wonach Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der Daten gewährleisten, einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen.

(ee) Privacy by design und privacy by default

14 Wesentliche Ausprägungen der in Art. 5 DSGVO normierten Grundsätze sind neben der Sicherheit der Datenverarbeitung nach Art. 32 DSGVO besonders die Verpflichtungen des Verantwortlichen zum Datenschutz durch Technikgestaltung (**data protection/**

---

[36] Dazu schon BVerfGE 65, 1 Rn. 148; so auch *Pötters* in Gola, DSGVO, 2. Aufl. 2018, Art. 5 Rn. 11.
[37] *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 218.
[38] *Schantz* in Wolff/Brink, BeckOK Datenschutzrecht, 39. Edition, DSGVO Art. 5 Rn. 25.
[39] *Wolff* in Wolff/Brink, BeckOK Datenschutzrecht, 39. Edition, Syst. A Rn. 44ff, 48.
[40] Dazu *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 216.
[41] *Herbst* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO Art. 5 Rn. 21.
[42] Vgl. dazu *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 221ff.
[43] Vgl. zur Kategorisierung *Wolff* in Wolff/Brink, BeckOK Datenschutzrecht, 39. Edition, Syst. A Rn. 64 ff.

„privacy" by design) und datenschutzfreundliche Voreinstellungen (**data protection/ „pricacy" by default**) gem. Art. 25 DSGVO.[44] Dabei muss der Verantwortliche technische und organisatorische Maßnahmen treffen, um die Umsetzung der datenschutzrechtlichen Grundsätze in allen Phasen umzusetzen und diese bereits bei der Gestaltung und Konzeption zu berücksichtigen.[45] Auch nach dem Grundsatz des Datenschutzes durch datenschutzfreundliche Voreinstellungen sollen standardmäßige Konfigurationen nur notwendige Datenerhebungen vorsehen, insbesondere Internet- und App-Anwendungen.[46]

[44] *Lang* in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, DSGVO Art. 25 Rn. 25; *Nolte/Werkmeister* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 25 Rn. 8.
[45] *Lang* in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, DSGVO Art. 25 Rn. 3.
[46] *Lang* in Taeger/Gabel, DSGVO BDSG TTDSG, 4. Aufl. 2022, DSGVO Art. 25 Rn. 68.

III. Status Quo: Grundlagen des Arbeitnehmerdatenschutzrechts

15 Im nächsten Schritt soll zunächst die **aktuelle Rechtslage** im Beschäftigungskontext anhand der rechtlichen Grundlagen des Arbeitnehmerdatenschutzes erläutert werden. Zur Bewertung des Projekts de lege lata stellen diese eine maßgebliche Rechtsgrundlage dar. Außerdem soll die aktuelle Rechtslage hinsichtlich technischer Leistungskontrollen am Arbeitsplatz kurz erläutert werden.

1. Grundlagen des Arbeitnehmerdatenschutzrechts

a) Interessenslagen im Beschäftigungskontext

16 Die enormen Mengen an – in einer Vielzahl von Fällen personenbezogenen – Daten im Beschäftigungskontext haben bedeutsame Auswirkungen auf die sich häufig konträr gegenüberstehenden Interessen von Arbeitgebern[47] und Arbeitnehmern.[48] **Arbeitgeber** haben ein berechtigtes Interesse daran, dass die von ihnen bereitgestellte Software nicht (zu privaten Zwecken) missbraucht wird und Arbeitnehmer nicht als „Einfallstor" für Viren und sonstige Schadsoftware (sog. „Social Engineering"[49]) oder die Weitergabe von Betriebs- und Geschäftsgeheimnissen benutzt werden. Zur Erfüllung gesetzlicher Compliance-Pflichten kann auch eine datenbasierte technische Leistungskontrolle in gewissem Maße legitim sein (hierzu siehe ausführlich sogleich). **Arbeitnehmer** haben gleichwohl ein höchst anerkennenswertes Interesse am Schutz ihrer personenbezogenen Daten als Ausdruck ihrer informationellen Selbstbestimmung. Zudem ist aufgrund der durch Weisungsgebundenheit und ökonomischen Abhängigkeit strukturell bedingten **Machtasymmetrie** zwischen Arbeitgeber und Arbeitnehmer ein erhöhter Schutzbedarf zugunsten von Arbeitnehmern geboten.[50]

b) Normative Grundlagen

17 Um das **Informations- bzw. Kontrollinteresse** des Arbeitgebers und das Interesse des Arbeitnehmers an effektivem Persönlichkeitsschutz in einen angemessenen Ausgleich zu bringen, bedarf es eines regulierenden Rechtsrahmens.[51] Das bestehende Beschäftigtendatenschutzrecht orientiert sich dabei an den erörterten gegenseitigen Interessen sowie vor allem der dargestellten Machtasymmetrie.

---

[47] Um Ungenauigkeiten zu vermeiden, wird bei der folgenden juristischen Darstellung weitgehend das generische Maskulin bzw. die in den Gesetzen genutzten Begriffe benutzt (z.B. der Verantwortliche, der Arbeitgeber). Dies sind gesetzliche Bezeichnungen, die alle Geschlechter gleichermaßen erfassen.
[48] Hierzu ausführlich *Braun* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 7 Rn. 1 ff.
[49] Vgl. hierzu BSI, Social Engineering – der Mensch als Schwachstelle, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html.
[50] So auch *Gräber/Nolden* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, BDSG § 26 Rn. 4.
[51] *Braun* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 7 Rn. 4.

Ein nationales Arbeitnehmerdatenschutzgesetz existiert trotz vereinzelter politischer Vorstöße[52] nicht. Auch die DSGVO enthält keine unmittelbaren Regelungen zum Datenschutz im Beschäftigungskontext. Vielmehr sieht **Art. 88 DSGVO** in Absatz 1 als sog. „Öffnungsklausel" vor, dass die Mitgliedstaaten Regelungen „hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext" treffen können. Art. 88 Abs. 2 DSGVO zieht solchen mitgliedstaatlichen Vorschriften Grenzen, die sich inhaltlich vor allem an der Menschenwürde und berechtigten Betroffeneninteressen orientieren.[53] 18

Mit **§ 26 BDSG** hat der deutsche Gesetzgeber von dieser Öffnungsklausel Gebrauch gemacht.[54] Danach dürfen personenbezogene Beschäftigtendaten „für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies […] erforderlich ist." Diese Vorschrift verdrängt zwar den allgemeineren Art. 6 Abs. 1 lit. f) DSGVO.[55] Allerdings entfaltet § 26 BDSG keine Sperrwirkung, sodass auch im Beschäftigungskontext Art. 6 Abs. 1 lit. f) DSGVO für die Verarbeitung personenbezogener Daten für andere als in § 26 BDSG genannte Zwecke herangezogen werden kann.[56] 19

§ 26 BDSG gilt aber nur dann, wenn Arbeitgeber bzw. Vorgesetzte **Beschäftigtendaten** verarbeiten und nicht für den umgekehrten Fall. Dies folgt einerseits aus dem Begriff des „Beschäftigten" in § 26 Abs. 8 BDSG, der neben besonderen Formen der Beschäftigung insbesondere Arbeitnehmer als vertraglich zu weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit Verpflichtete erfasst.[57] Ebenfalls sind leitende Angestellte in größeren hierarchischen Organisationsstrukturen vom Begriff des Beschäftigten und damit dem Schutzzweck der Norm erfasst.[58] Andererseits spricht auch der von Art. 88 DSGVO und § 26 BDSG intendierte Schutzzweck, dem spezifischen 20

---

[52] *Braun* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 7 Rn. 11, der auf den nicht durchgesetzten Gesetzesentwurf der Bundesregierung (BT-Drs. 17/4230) für ein Beschäftigtendatenschutzgesetz vom 15.12.2010 Bezug nimmt, das ab Februar 2012 im Parlament diskutiert wurde.

[53] *Wybitul*, Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO, NZA 2017, S. 413, 414; *Riesenhuber* in Wolff/Brink, BeckOK Datenschutzrecht, DSGVO Art. 88 Rn. 91; *Pauly* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, DSGVO Art. 88 Rn. 17.

[54] S. BT-Drs. 18/11325, S. 96. § 26 BDSG wurde in Umsetzung der DSGVO durch das sog. „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU" (DSAnpUG-EU) neu gefasst (s. BGBl. 2017 I Nr. 44, S. 2097) und orientiert sich weitgehend § 32 BDSG a.F., stellt aber eine etwas erweiternde Norm dar, s. so auch *Gola*, Der ‚neue' Beschäftigtendatenschutz nach § 26 BDSG n.F., BB 2017, S. 1462, 1464 und *Düwell/Brink*, Beschäftigtendatenschutz nach der Umsetzung der DSGVO, NZA 2017, S. 1081, 1083 ff.

[55] *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, S. 115, 116.

[56] *Gräber/Nolden* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, BDSG § 26 Rn. 10; *Gola* in Gola/Heckmann, BDSG, 13. Aufl. 2019, BDSG § 26 Rn. 3.

[57] *Gola* in Gola/Heckmann, BDSG, 13. Aufl. 2019, § 26 BDSG Rn. 14.

[58] *Riesenhuber* in Wolff/Brink, BeckOK Datenschutzrecht, 38. Edition, BDSG § 26 Rn. 22; BAG, Beschluss v. 09.04.2019 – 1 ABR 51/17, Auskunftsanspruch des Betriebsrats über (sensible) personenbezogene Arbeitnehmerdaten, NZA 2019, S. 1055 Rn. 34.

Machtungleichgewicht im Arbeitsverhältnis (s.o.) zu begegnen,[59] gegen eine Anwendbarkeit im umgekehrten Fall. Handelt es sich bei den Arbeitgebern um öffentliche Stellen der Länder ist für die Datenverarbeitung im Beschäftigungskontext bei entsprechender Regelung das jeweilige **Landesdatenschutzgesetz** maßgebliche Rechtsgrundlage.

21 Schließlich können im Einzelfall auch **kollektivrechtliche Regelungen** wie Tarifverträge oder Betriebsvereinbarungen im Beschäftigtenkontext zu berücksichtigen sein und eine Datenverarbeitung kann – wie § 26 Abs. 4 BDSG unter Hinweis auf Art. 88 Abs. 2 DSGVO ausdrücklich klarstellt – auch in zulässiger Weise auf Basis solcher Vereinbarungen möglich sein. Einige betriebliche Maßnahmen bedürfen allgemein (auch unabhängig von Betriebsvereinbarungen) der **Mitbestimmung des Betriebsrates**, z.B. nach § 87 Abs. 1 Nr. 1 BetrVG (Regelungen, die das Verhalten oder die Ordnung der Arbeitnehmer im Betrieb beeinflussen) oder § 87 Abs. 1 Nr. 6 BetrVG (Einführung technischer Überwachungssysteme), andere Vorschriften etwa sehen das **Recht** des Betriebsrates zur **Unterrichtung** und **Beratung** vor.

c) Spezifikationen für Datenverarbeitungen im Beschäftigungsverhältnis

22 Maßgebliche Vorschrift für die Verarbeitung von Arbeitnehmerdaten im Beschäftigungskontext ist daher **§ 26 BDSG**. Dieser kodifiziert in Abs. 1 und Abs. 3 insgesamt fünf Erlaubnistatbestände. Danach dürfen personenbezogene Daten von Beschäftigten verarbeitet werden, wenn dies für die Entscheidung über die Begründung oder anschließend für die **Durchführung bzw. Beendigung des Arbeitsverhältnisses erforderlich** ist. Daneben können sie verarbeitet werden, um einer gesetzlichen oder kollektivvertraglichen Verpflichtung nachzukommen (§ 26 Abs. 1 S. 1 BDSG). Unter bestimmten Voraussetzungen ist die Verarbeitung auch zur Aufdeckung von Straftaten im Beschäftigungsverhältnis zulässig (§ 26 Abs. 1 S. 2 BDSG). § 26 Abs. 3 BDSG regelt die Zulässigkeit der Verarbeitung sensibler Daten im Sinne des Art. 9 Abs. 1 DSGVO.

23 Darüber hinaus enthält § 26 BDSG die deklaratorische Feststellung, dass auch durch Einwilligung eine zulässige Beschäftigtendatenverarbeitung vorliegen kann.[60] An die **Freiwilligkeit** dieser Einwilligung sind aufgrund des dargelegten Machtungleichgewichts erhöhte Anforderungen zu stellen. Dies zeigt schon § 26 Abs. 2 S. 1 BDSG, wonach die **Umstände** der Einwilligungserteilung in die Verarbeitung personenbezogener Beschäftigtendaten sowie die dargestellte **Abhängigkeit** des Arbeitnehmers gesondert zu berücksichtigen sind. Nach § 26 Abs. 2 S. 2 BDSG, der insoweit ein Regelbeispiel

---

[59] *Braun* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 7 Rn. 11; *Gräber/Nolden* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, BDSG § 26 Rn. 4.

[60] Ausführlich zu den einzelnen Erlaubnistatbeständen ua *Gola* in Gola/Heckmann, BDSG, 13. Aufl. 2019, § 26 Rn. 18 ff.; *Maschmann* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, BDSG § 26 Rn. 17 ff.

darstellt,[61] kann Freiwilligkeit insbesondere dann vorliegen, „wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen“. Auch ist hinsichtlich der Freiwilligkeit stets der **Zeitpunkt der Einwilligung** zu betrachten. Es wird beispielsweise davon ausgegangen, dass Arbeitnehmer vor Unterzeichnung des Arbeitsvertrages einer höheren Drucksituation ausgesetzt sind als danach.[62] Dabei wird aufgrund der gesetzlichen Erlaubnistatbestände jedoch von einer untergeordneten Rolle der Einwilligung im Beschäftigungskontext ausgegangen.[63]

Eine wichtige – auch im Hinblick auf das Projekt relevante – Pflicht des Arbeitgebers als in der Regel datenschutzrechtlich Verantwortlichem findet sich schließlich in § 26 Abs. 5 DSGVO, wonach dieser geeignete Maßnahmen ergreifen muss, um die Einhaltung der Datenschutzgrundsätze aus Art. 5 DSGVO sicherzustellen. Dies betrifft insbesondere den Grundsatz der **Transparenz** aus Art. 5 Abs. 1 lit. a) DSGVO und die daraus erwachsenden **Informationspflichten** aus den Art. 12 ff. DSGVO. 24

2. Leistungskontrolle am Arbeitsplatz

Die Einhaltung des Transparenzgrundsatzes steht häufig im Konflikt mit (verdeckten) **Leistungs- und Verhaltenskontrollen** von Mitarbeitern am Arbeitsplatz. Diese können aus datenschutzrechtlicher Hinsicht grundsätzlich zulässig sein. Sie stehen aber stetig im Spannungsverhältnis von legitimen Arbeitgeberinteressen auf der einen und unzulässiger Totalüberwachung von Arbeitnehmern auf der anderen Seite. Anknüpfungspunkt ist das Kriterium der **Erforderlichkeit** in § 26 Abs. 1 S. 1 BDSG, wonach personenbezogene Daten dann verarbeitet werden dürfen, wenn dies zur Durchführung des Beschäftigungsverhältnisses erforderlich ist. Erforderlich ist eine Datenverarbeitung bereits bei Vorliegen berechtigter Interessen des Arbeitgebers, wobei dessen unternehmerische Freiheit und Organisationshoheit zu berücksichtigen sind.[64] 25

Die Prüfung nach der Zulässigkeit von Leistungskontrollen erfordert im Rahmen des Tatbestandsmerkmales der Erforderlichkeit dabei eine **zweistufige Verhältnismäßigkeitsprüfung**:[65] Auf der ***ersten Stufe*** ist die Erforderlichkeit einer Datenverarbeitung für die Interessen des Arbeitgebers zu prüfen. In diesem Rahmen ist zu kontrollieren, ob die Leistungs- und Verhaltenskontrolle tatsächlich zur Durchführung des Arbeitsverhältnisses im Sinne des § 26 Abs. 1 S. 1 BDSG erforderlich ist. **Legitime Arbeitgeberinteressen** an einer Kontrolle stellen beispielsweise die Erfüllung gesetzlicher Compliance-Pflichten dar. Beispielhaft genannt seien hier die Pflicht zur 26

---

[61] So auch *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 983 und *Riesenhuber* in BeckOK Datenschutzrecht, 38. Edition, BDSG § 26 Rn. 47.
[62] BT-Drs. 18/11325, 97; *Maschmann* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, BDSG § 26 Rn. 63.
[63] *Gola*, Der ‚neue‘ Beschäftigtendatenschutz nach § 26 BDSG nF, BB 2017, S. 1462, 1468.
[64] *Riesenhuber* in Wlff/Brink, BeckOK Datenschutzrecht, 38. Edition, BDSG § 26 Rn. 114.
[65] *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, S. 115, 117; *Gola* in Gola/Heckmann, BDSG, 13. Aufl. 2019, § 26 BDSG Rn. 69 ff.

Ergreifung geeigneter Maßnahmen und organisatorischer Vorkehrungen aus § 91 Abs. 2 AktG (Schaffung eines Überwachungssystems in der Aktiengesellschaft, um gefährdende Entwicklungen präventiv zu erkennen), die bei Missachtung gemäß §§ 30, 130, 9 OWiG mit empfindlichen Geldbußen geahndet werden kann.[66]

27 Die **Verhältnismäßigkeit** im engeren Sinne ist für den Einzelfall auf einer ***zweiten Stufe*** zu prüfen, auch wenn sich die Einzelfallbetrachtung oftmals schwierig darstellt. Immer zu berücksichtigen sind hierbei aber die datenschutzrechtlichen Betroffenenrechte sowie die aus dem Transparenzgrundsatz erwachsenden Informationspflichten des Arbeitgebers. In Rechtspraxis und -wissenschaft wurden gewisse Leitlinien entwickelt, in welchen Fällen eine derartige Leistungskontrolle zulässig ist. So soll es beispielsweise datenschutzrechtlich zulässig sein, die Nutzung zu dienstlichen Zwecken bereitgestellter IT-Systeme zu kontrollieren, wenn deren Privatnutzung verboten ist und die Kontrolle selbst verhältnismäßig ist.[67]

28 Unzulässig sind grundsätzlich – bislang sehr einschränkend als zulässig erachtete[68] - **heimliche und anonyme Mitarbeiterkontrollen**. Sie verletzen die informationelle Selbstbestimmung Betroffener, wenn sie **verdeckt** erfolgen und damit weder erkennbar noch abwendbar sind, selbst bei Einwilligung der Betroffenen.[69] Auch der Tatbestand des § 26 Abs. 1 S. 2 BDSG (Aufdeckung von Straftaten) soll als Legitimierung nicht ausreichen,[70] wobei auch das Gegenteil hinsichtlich der Aufdeckung schwerer Pflichtverletzungen vertreten wird.[71] Die Vertreter der Ansicht, dass § 26 BDSG für eine verdeckte Überwachung nicht ausreichen kann, erwägen einen Rückgriff auf Art. 6 Abs. 1 lit. f) DSGVO und eine Berücksichtigung der Rechtsprechung in der Interessensabwägung.[72] Auch der Einsatz sog. Keylogger und – in der Regel – eine offene präventive Videoüberwachung[73] am Arbeitsplatz sind unzulässig. Erfolgt eine Leistungs- und Verhaltenskontrolle mittels KI-Systemen, liegt in der Regel ein sog. **Profiling** nach Art. 4 Nr. 4 DSGVO vor und die Rechtmäßigkeit der Verarbeitung von Daten ist an Art. 22

---

[66] S. auch *Zöll* in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, § 26 BDSG Rn. 41, 42; *Stück*, Überwachungsmöglichkeiten des Arbeitgebers im Lichte aktueller Rechtsprechung, ArbR Aktuell 2018, S. 31.

[67] S. im Einzelnen ua *Fülbier/Splittgerber*, Keine (Fernmelde-)Geheimnisse vor dem Arbeitgeber?, NJW 2012, S. 1995; *Hoppe/Braun*, Arbeitnehmer-E-Mails: Vertrauen ist gut – Kontrolle ist schlecht, MMR 2010, S. 80; *Wybitul/Böhm*, E-Mail-Kontrollen für Compliance-Zwecke und bei internen Ermittlungen, CCZ 2015, S. 133; s. allgemein auch *Maschmann*, Führung und Mitarbeiterkontrolle nach neuem Datenschutzrecht, NZA-Beilage 2018, S. 115, 121 f.

[68] *Byers*, Die Zulässigkeit heimlicher Mitarbeiterkontrollen nach dem neuen Datenschutzrecht, NZA 2017, S. 1086, 1089.

[69] *Pauly* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, DSGVO Art. 88 Rn. 16.

[70] *Byers*, Die Zulässigkeit heimlicher Mitarbeiterkontrollen nach dem neuen Datenschutzrecht, NZA 2017, S. 1086, 1089; *Maschmann* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, BDSG § 26 Rn. 22 f.

[71] *Wedde*, juris PraxisReport Arbeitsrecht 17/2021, Anm. 6.

[72] *Byers*, Die Zulässigkeit heimlicher Mitarbeiterkontrollen nach dem neuen Datenschutzrecht, NZA 2017, S. 1086, 1089 f.

[73] *Stück*, Datenschutz = Tatenschutz?, CCZ 2020, S. 77, 81.

DSGVO zu messen. Dabei kann auch diese Kontrolle im Ausnahmefall zulässig sein, wenn sie eine Einzellösung darstellt, deren Letztentscheidung nicht ausschließlich automatisiert erfolgt.

B. Projektbezogene Darstellung

Im Folgenden soll das Projekt aus einer datenschutzrechtlichen Perspektive betrachtet werden. Im Fokus steht hierbei die **Inverse Transparenz Toolchain**. Die Toolchain wurde im Rahmen des Projekts durch die TU München entwickelt und setzt das Konzept der Inversen Transparenz bereits in ersten praxisrelevanten Darstellungen um. Daneben fließen zum Teil auch Ergebnisse der **Praxis-Laboratoriums, ein.** In diesem wurden in Kooperation mit der Software AG zwei Teams gebildet. Beide Teams erarbeiteten Use-Cases für Inverse Transparenz. Während das eine Team v.a. den Use Case Selbstauskunft umgesetzt hat (Nachvollziehbarkeit der auf Basis von iTrac getätigten Datenzugriffe durch Führungskräfte für Beschäftigte), hat das andere Team den Use Case der Expertensuche untersucht.[74]

I. Darstellung der Toolchain

29 Um die rechtlichen Herausforderungen des Einsatzes der Toolchain im Beschäftigungskontext zu erörtern ist eine kurze Zusammenfassung der **technischen Wirkungsweise** unerlässlich.

1. Der Grundsatz der „Transparency by Design“

30 Der Toolchain liegt zunächst das theoretische Konzept der **„Transparency by Design“**[75] als Weiterentwicklung des datenschutzrechtlichen Grundsatzes Privacy by Design zugrunde. Dieser Grundsatz gründet auf der Annahme, dass der bestehende Datenschutz im Softwaredesign den Herausforderungen entwickelter Tools nicht gerecht wird. Aus diesem Grund soll die Transparenz der Datennutzung im Interesse der Datensubjekte bereits bei der Softwarekonzeption berücksichtigt werden. Das Konzept von Transparency by Design beruht dabei direkt auf dem Konzept der Inversen Transparenz. Datensubjekte sollen die Möglichkeit erhalten, transparent über den Zugriff von Datennutzende auf ihre personenbezogenen Daten informiert zu werden.[76] Das entwickelte Design besteht aus insgesamt drei Schritten, die jeweils getrennt voneinander unterschiedliche Aufgaben wahrnehmen.

31 In einem **ersten Schritt** werden alle Datenzugriffe durch einen *Monitor* überwacht. Der **zweite Schritt** umfasst die Prüfung und Verifizierung der Authentizität der Datenzugriffe und die Speicherung in einem Nutzungsprotokoll. Dies erfolgt durch den *Verwahrer*. Damit das Datensubjekt auf die gespeicherten Daten zugreifen kann, macht in einem

---

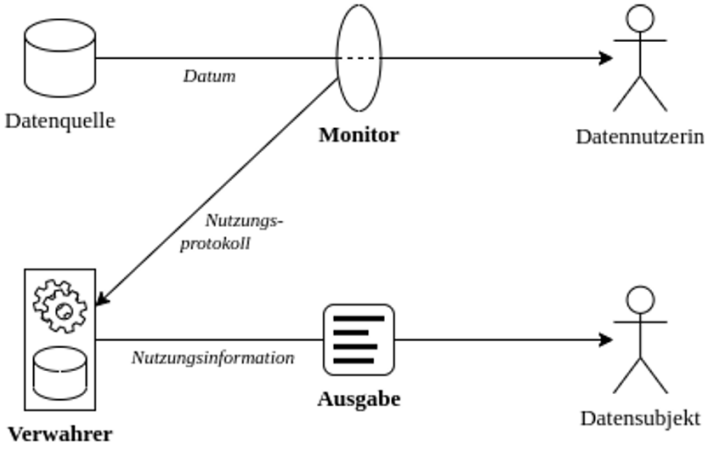
[74] Nähere Informationen zur Arbeit der beiden Teams finden sich im Forschungsreport zum Projekt (S. 70 ff.).

[75] *Zieglmeier/Pretschner*, Trustworthy transparency by design, Vorveröffentlichung auf arXiv. *arXiv:2103.10769*.

[76] **Datensubjekte** in diesem Kontext sind diejenigen Personen, auf deren personenbezogene Daten im Einzelfall zugegriffen wird, d.h. „Betroffene“ im Sinne der datenschutzrechtlichen Dogmatik, im Beschäftigungskontext in der Regel Beschäftigte. **Datennutzende** sind die auf die Daten Zugreifenden, im Beschäftigungskontext oftmals Arbeitgeber oder Vorgesetzte.

dritten Schritt die *Ausgabe* die Informationen über die gespeicherten Zugriffe dem Datensubjekt verfügbar.

Zur Verdeutlichung dieser drei konzeptionellen Schritte soll diese Abbildung[77] dienen:



2. „Zugriffe" und fälschungssicheres Nutzungsprotokoll

Bei den Auswirkungen dieser drei Schritte auf ein konkretes Softwaredesign wurden 32
insbesondere zwei kritische Fragestellungen herausgearbeitet. Zum einen stellt sich die Frage, wann ein für das Konzept relevanter **Zugriff** von Daten vorliegt. Daten bewegen sich in vielfältigsten Verarbeitungsgraden stetig zwischen verschiedenen Systemen. Allein das Starten einer datenbasierten Software oder das Aufrufen eines Dashboards kann daher bereits einen relevanten Zugriff auslösen. Dies kann vor dem Hintergrund einer sog. „**Umgebungsnutzung von Daten**" (*ambient usage*) problematisch sein. Öffnen Nutzer ein Tool für eine bestimmte Aktion (z.B. eine bestimmte Suche), öffnet sich zunächst das Dashboard mit vielen kleinen Anwendungsoberflächen und Fenstern und generiert eine Vielzahl – unnötiger – Datenzugriffe. Nach dem dargestellten Konzept soll aber nur der Zugriff von Datennutzende auf Daten von Datensubjekten einen relevanten und protokollierten Zugriff darstellen. Eine mögliche Lösung für diese Problematik erscheint darin, Datennutzende die Zugriffe durch technische Implementierungen bewusst zu machen. Orientiert man sich am Beispiel des Dashboards wird dabei vorgeschlagen, man könne Analysen nur auf explizite Anfrage freischalten und ansonsten verbergen.[78]

---

[77] „Transparentmachen von Datenzugriffen durch ein konzeptionelles Framework für Transparency by Design", *Zieglmeier/Pretschner,* Trustworthy transparency by design, 2021, Vorveröffentlichung auf arXiv. *arXiv:2103.10769*.

[78] Die technische Implementierung der Analyse auf explizite Anfrage ist beim Use Case des *Jira*-Dashboards technisch prinzipiell möglich und wurde auch genau so in den Anwendungsbeispielen umgesetzt. Allerdings betraf das nur die Analysen, die für das Praxislaboratorium bereitgestellt wurden und nicht die bereits bei Jira/iTrac vorhandenen Analysewerkzeuge.

33 Zum anderen ist es gleichwohl im Sinne von Datennutzenden und -subjekten, die Vertraulichkeit und Integrität des Nutzungsprotokolls sicherzustellen. Ein **fälschungssicheres Nutzungsprotokoll** ist für die Anwendung und das intendierte Ergebnis des Transparency by Design essentiell. Zur Gewährleistung der Integrität werden dabei vor allem zwei technische Lösungen extrahiert und vorgeschlagen:

- Bei den sogenannten *Software Guard Extensions* (SGX)[79] von *Intel* wird eine abgeschottete Umgebung auf Prozessoren mittels kryptografischer Verfahren erzeugt. Die Anwendung dieser Software führe auch auf nicht kontrollierbaren Systemen zu Sicherheit vor Manipulation.
- Alternativ werden auch *Blockchain*[80]-Lösungen vorgeschlagen. Systemnutzer speichern eine Kopie des Nutzungsprotokolls als Blockchain. Ein dem Datensubjekt zugewiesener sog. „Knoten" erhält die Zugriffsanfrage und erstellt einen Protokolleintrag, den er bei Zugriffserteilung an das Netzwerk sendet.

3. Use-Case: Die Toolchain der Inversen Transparenz in der Praxis

34 Zur Ermöglichung von Transparency by Design wurde zur konkreten Anwendung der Toolchain bei der Projektpartnerin Software AG das Projektmanagement- und Optimierungs-Tool *Jira*[81] ausgemacht. Die drei Konzeptionsschritte wurden dabei als selbständige Web-Services erstellt, die auf unternehmenseigenen Servern eingesetzt werden können. In der praktischen Anwendung hat das Unternehmen die Kontrolle über und den Zugriff auf die Server, auf denen die Toolchain eingesetzt wird.

35 In Anlehnung an die obige Abbildung zum Konzept der Transparency by Design soll die folgende Abbildung[82] die Toolchain im konkreten Anwendungsfall darstellen:

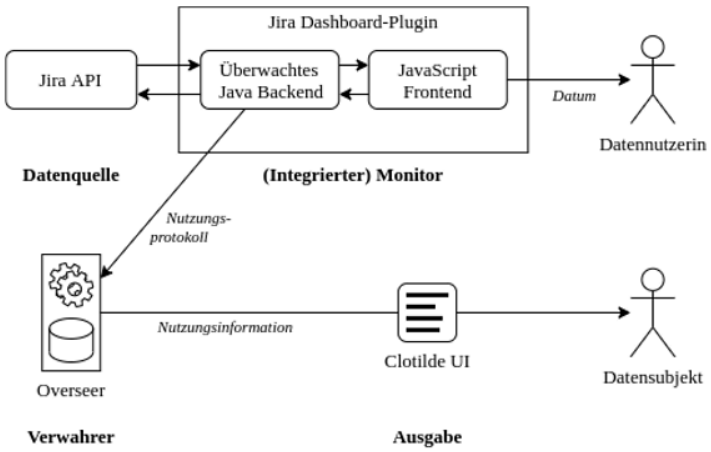
---

[79] Zu beachten ist, dass das regelmäßige Auftreten von Sicherheitslücken zur Deaktivierung in Prozessoren der 11. und 12. Generation der Prozessoren geführt hat, vgl. https://www.heise.de/news/UHD-Blu-rays-lassen-sich-nicht-mehr-auf-neuen-PCs-wiedergeben-SGX-deaktiviert-6326346.html: So ist zu empfehlen, eine vergleichbare Lösung einzusetzen.

[80] Vgl. hierzu *Zieglmeier*/Gabriel, GDPR-Compliant Use of Blockchain for Secure Usage Logs, 2021, S. 313-320.

[81] *Jira* ist eine Webanwendung des Entwicklers Atlassian und dient dem operativen Projektmanagement sowie der Fehlerverwaltung und Problembehandlung. Ursprünglich vor allem in der Softwareentwicklung eingesetzt, wird *Jira* zunehmend auch im nichttechnischen Bereich genutzt. Dabei kann es neben dem Projektmanagement vor allem auch zur Prozessoptimierung eingesetzt werden.

[82] „Instantiierung des Konzepts für Transparency by Design mit Web-Services am Anwendungsbeispiel *Jira* Software", *Zieglmeier/Pretschner,* Trustworthy transparency by design, 2021, Vorveröffentlichung auf arXiv. *arXiv:2103.10769*.



Ausgangspunkt des **Use-Cases** ist dabei das Software-Tool *Jira*, das vor allem der Nachverfolgung von Problemen dient. Probleme stellen dabei „Arbeitsaufgaben“ dar, die von jedem Systemnutzer erstellt, zugewiesen und mit externen Vorgängen wie beispielsweise Links oder Dateien versehen werden können. Ein solches „Ticket“ kann von den Usern auch kommentiert werden. 36

Daran anknüpfend wurden der **Verwahrer** (*Overseer)*, dem die Aufgabe des Verwahrers zur Verifizierung und Speicherung des Nutzungsprotokolls zukommt und das Web-Frontend *Clotilde UI* als Benutzeroberfläche entwickelt, das als Ausgabe die Zugriffe den Datensubjekten zur Verfügung stellt. Der ***Monitor*** soll insbesondere die Datennutzung nachverfolgen und überwachen. Im Anwendungsfall wurde dieser Monitor in *Jira*-Dashboard-Plugins in überwachten Java-Backends integriert und dadurch in die Software implementiert. Er soll dabei nur der **Sichtbarmachung** der Datennutzung dienen, das installierte Plugin war in seiner Anwendung nur lesend tätig. Jede Anfrage an das JavaScript-Frontend (die Anwendungsoberflächen bzw. Fenster des Dashboards) löst dann automatisch eine Protokollierung beim *Verwahrer* (Overseer) aus. Dieser überprüft und speichert die Nutzungsinformationen und stellt diese der *Ausgabe* (Clotilde-UI) zur Verfügung und ist daher als Back-End der Toolchain zu betrachten. Das (Web-)Front-End der Toolchain stellt schließlich die Display-App Clotilde UI als ***Ausgabe*** dar, über die Datensubjekte Informationen über die Datenzugriffe erhalten. Die Datensubjekte als Nutzende interagieren ausschließlich mit der Ausgabe. Stellen die Datensubjekte eine Anfrage an das Front-End des Transparency Frameworks, also die *Ausgabe*, überprüft der *Verwahrer*, ob das Datensubjekt im Einzelfall hierzu berechtigt ist. 37

II. Rechtliche Stellungnahme

38 Die auf dem Konzept des Transparency by Design entwickelte Toolchain und ihre Anwendung vor dem Hintergrund Inverser Transparenz in der Arbeitswelt soll nun in einem **datenschutzrechtlichen Kontext** näher betrachtet werden. Hierbei sollen insbesondere **die maßgeblichen rechtlichen Herausforderungen** unter Berücksichtigung der Umsetzung und der Ergebnisse im Forschungsprojekt extrahiert werden

1. Datenverarbeitungen der Toolchain

Dafür sollen zunächst die relevanten Datenverarbeitungen bei Anwendung der Toolchain identifiziert werden.

a) Die Verarbeitung personenbezogener Daten als Voraussetzung der Anwendbarkeit des Datenschutzrechts

39 Der sachliche Anwendungsbereich der DSGVO ist gem. Art. 2 Abs. 1 DSGVO für die ganz oder teilweise automatisierte sowie nichtautomatisierte Verarbeitung[83] personenbezogener Daten[84] eröffnet. Der Begriff der **Verarbeitung** ergibt sich aus Art. 4 Nr. 2 DSGVO, wonach eine Verarbeitung als jeder **mit oder ohne Hilfe automatisierter Verfahren** ausgeführten **Vorgang** oder jede **Vorgangsreihe** in diesem Kontext **im Zusammenhang mit personenbezogenen Daten** definiert ist. Nach Art. 4 Nr. 2 DSGVO fallen insbesondere das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung unter den Begriff. Diese Aufzählung ist allerdings nicht abschließend,[85] sodass unter die sehr weit gefasste Definition auch weitere auf Daten einwirkende Vorgänge fallen. In **Zweifelsfällen** sollte wegen dieser weiten Begriffsbestimmung von einer „Verarbeitung“ ausgegangen werden.[86] Das Vorliegen einer Verarbeitung ist schließlich allein nach den objektiven Kriterien des Art. 4 Nr. 2 DSGVO zu bestimmen und ein – gegebenenfalls entgegenstehender – subjektiver Verarbeitungswille irrelevant.[87]

---

[83] Nach Art. 2 Abs. 1 DSGVO sind auch nichtautomatisierte Verarbeitungen maßgeblich, wenn sie in Dateisystemen gespeichert sind oder gespeichert werden sollen.
[84] Zum Begriff und Erläuterung des personenbezogenen Datums s.o. A.II.3.
[85] *Herbst* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO Art. 4 Rn. 20.
[86] *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 186.
[87] *Arning/Rothkegel* in Taeger/Gabel, DSGVO - BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DSGVO Rn. 67.

b) Die Toolchain als automatisiertes Verfahren

Auch wenn eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO sowohl bei automatisierten als auch nichtautomatisierten Verfahren vorliegen kann, sei hier zur Klarstellung im Rahmen der Subsumtion erläutert, dass es sich bei der Inversen Transparenz Toolchain und ihren drei konzeptionellen Komponenten um ein **automatisiertes Verfahren** handelt. Darunter versteht man die Verarbeitung von Daten mithilfe technischer Datenverarbeitungsanlagen.[88] Da die Komponenten des Frameworks als Web-Services auf Unternehmensservern genutzt werden, liegt unproblematisch ein automatisiertes Verfahren vor. 40

c) Zusammenhang mit personenbezogenen Daten

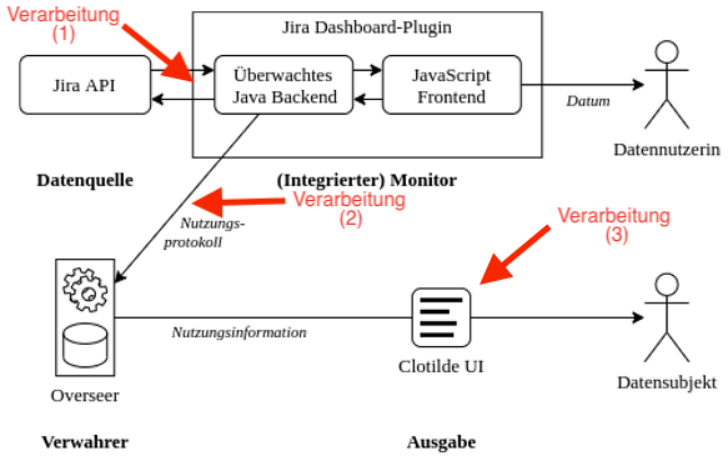
Im Zentrum der Toolchain steht die Information, wann Datennutzende auf personenbezogene Daten von Datensubjekten **zugegriffen** haben. Diese Information über den Datenzugriff durch Datennutzende – im Beschäftigungskontext in der Regel Arbeitgeber und Vorgesetzte – stellt selbst ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DSGVO dar. Wie bereits dargestellt ist für diese Einordnung die Identifizierung bzw. Identifizierbarkeit einer Person durch die jeweilige Information maßgeblich. Eine Person ist identifiziert, wenn die Informationen direkt auf eine Person schließen lassen.[89] 41

Kern des Konzepts der Inversen Transparenz und der im Projekt auf *Jira* angewandten Toolchain ist es gerade, im Sinne der **Datennutzungstransparenz** auf Daten zugreifende Systemteilnehmer zu identifizieren. Die hinter dem Zugriff stehende Person wird durch ihren Namen oder zumindest eine Kennung – unabhängig davon in welcher Softwareanwendung das Tool eingesetzt wird - eindeutig identifiziert.[90] Die Information über den Zugriff und den hinter dem Zugriff stehenden Arbeitgeber bzw. Vorgesetzten stellen somit ein personenbezogenes Datum nach Art. 4 Nr. 1 DSGVO dar. 42

[88] *Herbst* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO Art. 4 Rn. 17.
[89] *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 120 mwN.
[90] Zur Identifizierbarkeit ausführlich *Schild* in BeckOK Datenschutzrecht, 38. Edition, DSGVO Art. 4 Rn. 14 ff.

d) Verarbeitungen in der Toolchain

43 Auf Basis der technischen Erläuterungen und Vorgänge in der Inverse Transparenz Toolchain lassen sich schließlich insgesamt **drei Verarbeitungen** personenbezogener Daten im System identifizieren, die jeweils getrennt voneinander erfolgen:



(Modifizierung der ursprünglichen Abbildung[91] durch die Autoren)

(aa) Verarbeitung (1): Nachverfolgung der Datennutzung durch den Monitor

44 Bereits die **Nachverfolgung** der jeweiligen Datennutzung durch den **Monitor** stellt eine datenschutzrechtrechtlich relevante Verarbeitung dar. Zwar erscheint dies auf den ersten Blick nicht eindeutig, da der Monitor vor allem lesend tätig ist und insbesondere dafür sorgt, dass eine Nutzungsanfrage (z.B. durch einen Klick auf dem *Jira*-Dashboard) innerhalb der genutzten Software automatisch zu einer Protokollierung beim Verwahrer führt. Er dient daher vor allem der Sichtbarmachung von Datenzugriffen in der Software für den Verwahrer. Wie bereits ausführlich dargestellt erfolgt die Implementierung des Monitors in die Anwendungssoftware über ein Plugin, das in das Java-Backend der Software integriert wird.

45 Eine Verarbeitung im datenschutzrechtlichen Sinne liegt jedoch trotz oder gerade auch wegen der „bloße[n] Sichtbarmachung“ vor. Eine Verarbeitung umfasst i.W. alle Vorgänge, die personenbezogene Daten verwenden oder im Zusammenhang mit Daten stehen[92], auch das Erheben und Erfassen von Transaktionsdaten[93] oder das Auslesen.[94] Betrachtet man die Funktionsweise des Monitors, basiert diese auf zwei Komponenten. Er **überwacht** die Software auf der Suche nach Datenzugriffen. Für diese Überwachung

---

[91] „Instantiierung des Konzepts für Transparency by Design mit Web-Services am Anwendungsbeispiel *Jira* Software, *Zieglmeier/Pretschner*, Trustworthy transparency by design, 2021, Vorveröffentlichung auf arXiv. *arXiv:2103.10769*.
[92] *Heckmann/Scheurer* in jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 20.
[93] *Klabunde* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, DSGVO Art. 4 Rn. 23.
[94] *Heckmann/Scheurer* in jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 20.

müssen notwendigerweise alle anfallenden Daten ausgelesen werden. Erfolgt eine Zugriffsanfrage, wird diese durch den Monitor „**abgefangen**“ und an den Verwahrer weitergeleitet. Der Monitor wird daher aktiv tätig, indem er die erforderlichen Daten über die Datennutzung (erstmalig) beschafft und an den Verwahrer weiterleitet. Aus diesen Gründen liegt jedenfalls unter Zugrundelegung des nicht abschließenden und weit auszulegenden Verarbeitungsbegriffs im Zweifelsfall[95] eine **Erhebung** personenbezogener Daten nach Art. 4 Nr. 2 Alt. 1 DSGVO vor.[96]

(bb) Verarbeitung (2): Speicherung der Datennutzung durch den Verwahrer

Der Verwahrer (Overseer) überprüft und speichert schließlich die Informationen über die Datennutzung im Nutzungsprotokoll in der Toolchain. Durch die **Speicherung** liegt – unabhängig der konkreten Ausgestaltung des Nutzungsprotokolls - eine weitere Verarbeitung nach Art. 4 Nr. 2 Alt. 5 DSGVO vor.[97] 46

(cc) Verarbeitung (3): Verfügbare Informationen durch die Ausgabe

Die für das Konzept der Inversen Transparenz und die Auswirkungen auf das Beschäftigungsverhältnis relevanteste Datenverarbeitung ist schließlich das **Verfügbarmachen** der Informationen über den Datenzugriff für das Datensubjekt durch die Ausgabe (Clotilde UI). Ausgelöst durch die **Abfrage** des oder der Zugreifenden durch das Datensubjekt (Art. 4 Nr. 2 Alt. 9 DSGVO), d.h. die gezielte Suche anhand bestimmter Kriterien (nach dem Zugriff),[98] prüft der Verwahrer dann die Berechtigung und die Ausgabe stellt die Informationen über den Zugriff dem Datensubjekt zur Verfügung. 47

(dd) Zusammenfassung

Somit finden innerhalb der Inversen Transparenz Toolchain insgesamt drei Datenverarbeitungen nach Art. 4 Nr. 2 DSGVO statt. Der Monitor **erhebt** durch das Abfangen der Nutzungsanfrage Daten über den Zugriff, der Verwahrer **speichert** diese Daten in einem Nutzungsprotokoll während die Ausgabe diese Daten **abfragt** und dem Datensubjekt zur Verfügung stellt. 48

2. Grundsätze der Datenverarbeitung

Im Folgenden ist das Tool im Hinblick auf die Umsetzung der oben beschriebenen bußgeldbewehrten Grundsätze der Datenverarbeitung einzuordnen.

---

[95] *Heckmann/Scheurer* in jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 186.
[96] *Arning/Rothkegel* in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 4 DSGVO Rn. 70.
[97] Zur Speicherung s. *Herbst* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO Art. 4 Rn. 24.
[98] *Arning/Rothkegel* in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 4 DSGVO Rn. 70.

a) Grundsatz der Transparenz

(aa) Transparenz

49 Nach dem **Grundsatz der Transparenz** gem. Art. 5 Abs. 1 lit. a) Var. 3 DSGVO sollen Daten in einer nachvollziehbaren Weise verarbeitet werden, wonach v.a. heimliche oder für die betroffene Person unbekannte Verarbeitungen ausgeschlossen werden sollen.[99] Nach Erwägungsgrund 39 S. 2 der DSGVO soll für natürliche Personen Transparenz im Hinblick auf die Verarbeitung, Erhebung, Einsehung oder Verwendung der sie betreffenden personenbezogenen Daten bestehen, wobei sich daraus konkretisierte Transparenzpflichten aus den Informations- und Auskunftsrechten gem. Art. 12-15 DSGVO, aber auch Pflichten im Hinblick auf data protection by design/default nach Art. 25 DSGVO ergeben.[100] Der Grundsatz steht vor dem Hintergrund, dass eine souveräne Ausübung der informationellen Selbstbestimmung und der Betroffenenrechte nur möglich ist, wenn die betroffenen Personen überhaupt erst Art und Umfang der über sie erhobenen Daten überblicken können.[101] Konkret ist darauf zu achten, dass der Verantwortliche gem. Art. 12 Abs. 1 S. 1 DSGVO geeignete Maßnahmen trifft, um den betroffenen Personen alle relevanten Mitteilungen im Hinblick auf die Verarbeitung in präziser, transparenter, verständlicher und leicht zugänglicher Form in einfacher Sprache zu übermitteln. Nach Erwägungsgrund 39 S. 4 der DSGVO betrifft dies u.a. Informationen über die Identität des Verantwortlichen, die Zwecke der Verarbeitung, Risiken sowie die Rechte der Betroffenen auf Auskunft über die erhobenen Daten. Bei der weiteren Umsetzung des Tools ist dabei zu achten, dass neben der Informationspflichten auch die Auskunftsrechte der betroffenen Person nach Art. 15 Abs. 1 DSGVO umgesetzt werden können.[102]

(bb) Inverse Transparenz

50 Im Hinblick auf den **Schutzzweck** der Vermeidung **heimlicher** und **unbekannter Datenverarbeitungen** ist das Konzept der Inversen Transparenz Toolchain positiv zu bewerten. Durch die wechselseitige Transparenz und aktive Einbeziehung der Mitarbeitenden in den Informationsfluss können die Arbeitnehmerinnen und Arbeitnehmer potentielle Datenzugriffe durch Führungskräfte oder andere Mitarbeitende jederzeit transparent nachvollziehen und einen möglichen Missbrauch oder heimliche Datenverarbeitungen frühzeitig bemerken oder überhaupt erst sichtbar machen.

51 Besonders das Konzept, Transparenz bereits im Softwaredesign zu berücksichtigen (transparency by design[103]) kann so – analog zu den Grundsätzen privacy by design und

---

[99] *Herbst* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 5 Rn. 18.
[100] Vgl. Erwägungsgrund 39 S. 3; *Herbst* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art. 5 Rn. 19.
[101] Dazu schon BVerfGE 65, 1 Rn. 148, auch *Bäcker* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, Art.
[102] *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl., Kap. 9 Rn. 426.
[103] Vgl. *Zieglmeier/Pretschner*, Trustworthy transparency by design., S. 4

privacy by default – dafür sorgen, dass der in Art. 5 Abs. 1 lit. a) Var. 3 DSGVO normierte Transparenzgedanke noch mehr in den Vordergrund gerückt wird und bereits bei der Softwareentwicklung und Implementierung mitgedacht wird. Durch die **so hergestellte Transparenz** und Kenntnis über die Datenerhebungen werden die betroffenen Arbeitnehmerinnen und Arbeitnehmer von Anfang an in die Lage versetzt, ihr Recht auf informationelle Selbstbestimmung und die Betroffenenrechte der DSGVO souverän und selbstbestimmt auszuüben[104], sodass sie nicht erst durch die auszuübenden Auskunftsrechte in diese Lage versetzt werden können, sondern „by design".

Der potentielle Einfluss zeigt sich auch **in Erkenntnissen des Praxislaboratoriums** mit dem Projektpartner der Software AG. Dort testete eines der Teams das Erprobungsfeld der Inversen Transparenz am Beispiel einer modifizierten Expertensuche am Softwaretool *iTrac*. Dabei ergab sich in zu Beginn des Praxislaboratoriums durchgeführten Interviews u.a. die Antwort, dass diese Daten bis dahin überwiegend Führungskräfte nutzten und gerade nicht die Mitarbeitenden zur Verbesserung der eigenen Arbeit.[105] Dies ließ sich u.a. auf Ängste und Vorbehalte zur Gruppen- bzw. Leistungskontrolle und Leistungsdruck, aber auch auf fehlendes Wissen über anfallende Daten zurückführen.[106] Auch wissen viele Beschäftigte nicht, dass sie grundsätzlich Zugriff auf die von iTrac generierten und zur Verfügung stehenden Daten haben. In der Praxis haben viele Beschäftigte auch weder Zeit noch Raum, sich damit zu beschäftigen, wie sie die Daten gewinnbringend für sich nutzen können. Langjährige Mitarbeiter gaben dabei an, trotz Vereinbarungen im Betriebsrat zum Ausschluss der Verwendung von *Jira*/*iTrac*-Daten zur Leistungskontrolle, zu fragen, welche Daten durch das Tool tatsächlich erhoben werden und waren unsicher, wie diese letztlich verwendet werden können.[107] Die ersten Befunde im Projekt legen nahe, dass Inverse Transparenz das Potenzial hat, Ängste und Unsicherheit zu verringern und das Empowerment der Beschäftigten im Umgang mit Daten zu stärken.[108] 52

Gleichwohl gilt zu beachten, dass die dargestellten Ansätze zwar durchweg positiven Einfluss auf den Grundsatz der Transparenz nach Art. 5 Abs. 1 lit. a) Var. 3 DSGVO haben können. Eine **zunächst rechtswidrige** Datenverarbeitung wird durch die Einführung von mehr **Transparenz** aber **nicht rechtmäßig**. Die Rechtmäßigkeit beurteilt sich für nicht sensible personenbezogene Daten nach Art. 6 DSGVO, wobei nach dem Verbotsprinzip mit 53

---

[104] Dazu Fn. 102.

[105] Das war ein zentrales Ergebnis der qualitativen Interviews bei der Software AG, die das ISF München unter Beteiligung der Kolleg/innen der LMU und TU zu Beginn des Praxislaboratoriums geführt hat. Dabei wurden sowohl mit Expertinnen und Experten (Datenschutzbeauftragter, HR, BR, Führungskräfte) als auch Beschäftigten unterschiedlicher Bereiche, Alter- und Qualifikationsstufen (Support, Entwicklung, R&D) über 20 qualitative Tiefeninterviews geführt (Zeitraum Mai - Juni 2019).

[106] Diese Stimmen ergaben sich im Rahmen des Projekts aus qualitativen Analysen der Umfrage an *iTrac*-Nutzer in Deutschland.

[107] Dies ergibt sich aus einer im Rahmen des Projekts durchgeführten Reportage.

[108] Vgl. *Kämpf/Vogl/Boes*, Forschungsreport Inverse Transparenz, S. 31.

Erlaubnisvorbehalt ein einschlägiger Rechtfertigungstatbestand gegeben sein muss. Liegt kein Erlaubnistatbestand vor, bleibt die Verarbeitung rechtswidrig, auch wenn Inverse Transparenz hergestellt wird oder die allgemeine Transparenz erhöht wird. Sonst könnte die eingeführte Transparenz letztlich zum Nachteil der Arbeitnehmerinnen und Arbeitnehmer und ihrer informationellen Selbstbestimmung führen, indem sich das Machtungleichgewicht in § 26 BDSG weiter manifestiert und mehr Leistungskontrollen oder Datenerhebungen „durch Transparenz" gerechtfertigt würden. Die Toolchain und eine gegebenenfalls erhöhte inverse Transparenz dürfen nicht als Rechtfertigungsgrundlage für noch mehr Datenverarbeitungen gesehen werden.

b) Grundsatz der Datenminimierung

(aa) Voraussetzungen der Datenminimierung

54 Nach dem **Grundsatz der Datenminimierung** gem. Art. 5 Abs. 1 lit. c) DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Durch die Bezugnahme auf den Zweck ergänzen sich die Grundsätze der Datenminimierung der Zweckbindung wechselseitig, wobei der Grundsatz nicht absolut zu verstehen ist, sondern je nach gewähltem Zweck auch umfassendere Datenverarbeitungen umfassen kann.[109] Die Tatbestandsmerkmale der Erheblichkeit, der Beschränkung auf das notwendige Maß sowie der Angemessenheit geben eine dreistufige Prüfung vor, die im Wesentlichen einer Verhältnismäßigkeitsprüfung entspricht.[110] Die erhobenen Daten müssen sich auf den festgelegten Zweck beziehen, geeignet sein, ihn zu fördern und jedenfalls in qualitativer sowie quantitativer Hinsicht solche Daten ausnehmen, ohne die der Zweck auch erreicht werden kann.[111]

(bb) Datenminimierung im Kontext Inverser Transparenz

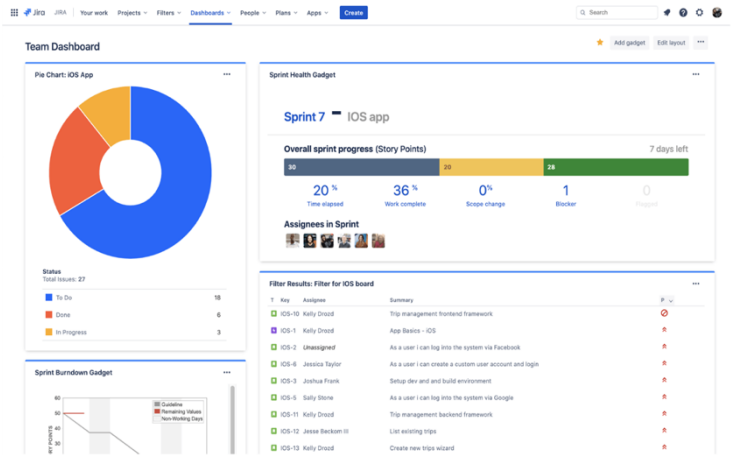
55 Fraglich ist zunächst, ob es aufgrund des dargestellten Grundsatzes der Datenminimierung überhaupt einer weiteren Datenverarbeitung durch die Implementierung bedarf. Die Erfüllung des Grundsatzes könnte besonders dann im Zweifel stehen, wenn es um Datenverarbeitungen geht, die rechtlich bereits ohnehin zulässig sind, wie z.B. bei bestimmten Leistungskontrollen oder anderen Datenverarbeitungen des Arbeitgebers bei gesetzlichen Regelungen (u.a. Compliance-Pflichten) oder Vereinbarungen (z.B. Betriebsvereinbarungen[112]). Dabei könnte die zusätzliche Implementierung des Tools den **Bedarf** mit Blick auf die Datenminimierung in Frage stellen.

---

[109] Je nach Zweck können sogar Big-Data Anwendungen darunterfallen, vgl. auch *Herbst* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, DSGVO Art. 5 Rn. 56.
[110] *Schantz* in Wolff/Brink, BeckOK Datenschutzrecht, 39. Edition, DSGVO Art. 5 Rn. 24ff.
[111] *Herbst* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, DSGVO Art. 5 Rn. 57.
[112] Beim Praxispartner waren Leistungskontrollen aufgrund der von *Jira*/*iTrac* erhobenen Daten dagegen beispielsweise durch Betriebsvereinbarung ausgeschlossen.

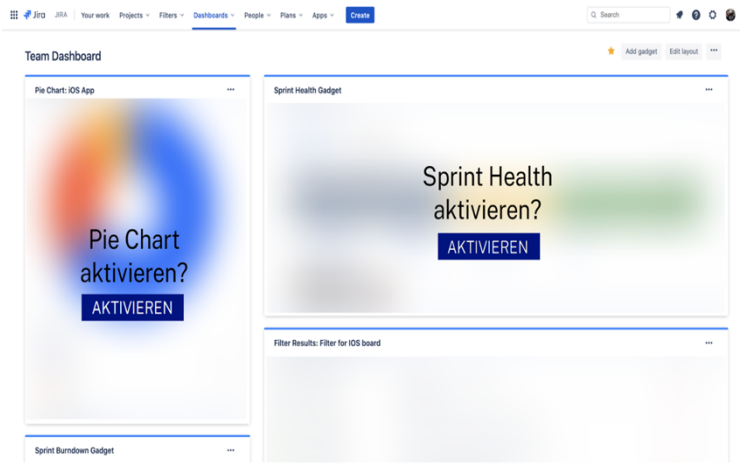
Gleichwohl ist im Rahmen des Grundsatzes der Datenminimierung auch der **Zweck** der Implementierung der Toolchain zu berücksichtigen. Dieser besteht darin, die Mitarbeitenden im Arbeitskontext zur gleichberechtigten und aktiven Datennutzung zu empowern.[113] Das erfolgt durch die Herstellung von Transparenz in beide Richtungen, sodass die Informationsherrschaft nicht mehr alleine bei den Führungskräften liegt, sondern auch bei den Mitarbeitenden.[114] Dadurch soll das Vertrauen der Mitarbeitenden in die Daten und die **souveräne Ausübung der informationellen Selbstbestimmung** am Arbeitsplatz gestärkt werden, indem in einem ersten Schritt möglicher Missbrauch überhaupt sichtbar gemacht werden kann und Kenntnisse über die über sie erhobenen Daten geschaffen werden können. Bei der Frage inwieweit die Einführung der Inversen Transparenz tatsächlich geeignet ist, diesen Zweck zu fördern, ist auf die soziologischen Erkenntnisse und ggfs. weitere notwendige Forschung abzustellen, da dies aus juristischer Perspektive nicht abschließend beurteilt werden kann.[115] In einem letzten Schritt ist zu prüfen, ob die Daten auf das angemessene Maß beschränkt sind. Für die Erhebung gezielter Zugriffe, wie z.B. beim Use Case der Expertensuche, ist die Speicherung der Zugriffe für den Zweck erforderlich und auch nicht durch ungenauere Daten oder gar anonyme Daten umzusetzen. Problematisch ist dagegen die garantierte Protokollierung von ausschließlich relevanten Zugriffen. Hier müsste sichergestellt werden, dass Zugriffe auf Menüfunktionen oder für den Zweck nicht erforderliche Funktionen, keine Protokollierung auslösen. Im Hinblick auf umfassende Dashboards, die sich beim Öffnen solcher Tools wie *Jira* zeigen und die viele Informationen auf einen Blick präsentieren, könnten sonst viele Informationen protokolliert werden (sog. Umgebungsnutzung von Daten oder *„ambient usage“*, s.o.), wenngleich der Nutzende nur einzelne Informationen zielgerichtet betrachten will. **56**

[113] *Kämpf/Langes*, Künstliche Intelligenz in der Arbeitswelt. Erste Befunde einer empirischen Bestandsaufnahme, 2022; so auch *Kämpf/Vogl/Boes*, Forschungsreport Inverse Transparenz, S. 31.
[114] Vgl. *Kämpf/Vogl/Boes*, Forschungsreport Inverse Transparenz, S. 29 f.
[115] Die ersten Erkenntnisse aus Umfragen am Use-Case der Skilldatenbank ergaben hier ein gemischtes Ergebnis mit zwei im Wesentlich zu identifizierbaren Gruppen der Skeptiker sowie der tendenziellen Befürworter.



(Beispiel-Dashboard von Jira, Quelle: atlassian.com)[116]

57 Um die Daten auf das angemessene Maß zu beschränken und so der Datenminimierung vollumfänglich gerecht zu werden, müsste darauf geachtet werden, dass nur relevante Datenzugriffe eine Protokollierung auslösen. Hierzu wurde im Projekt ein möglicher Lösungsvorschlag eines modifizierten Dashboards entwickelt, das sich diesem Problem annimmt und Informationen ausblendet, solange sie nicht aktiv angesteuert werden.



(Modifiziertes Beispiel-Dashboard von Jira, Quelle atlassian.com)[117]

Rechtlich ist zu empfehlen, das Konzept bei der Umsetzung und Implementierung der Toolchain in weitere Programme von Anfang an zu berücksichtigen und das Konzept praktisch umzusetzen.

---

[116] Diese Grafik ist entnommen aus *Pretschner/Zieglmeier*, Forschungsreport Inverse Transparenz, S. 49.

[117] Diese Grafik ist entnommen aus *Pretschner/Zieglmeier*, Forschungsreport Inverse Transparenz, S. 49.

c) Grundsatz der Vertraulichkeit und Integrität

Personenbezogene Daten müssen derart verarbeitet werden, dass eine **angemessene Sicherheit der Daten** gewährleistet ist.[118] Dies statuiert der Grundsatz der Vertraulichkeit und Integrität in Art. 5 Abs. 1 lit. f) DSGVO und umfasst die Verpflichtung zu technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten vor Zerstörung, Beschädigung oder unbefugtem Zugriff.[119] Nach Art. 32 Abs. 1 DSGVO sind dabei Maßnahmen für ein **angemessenes Schutzniveau** zu treffen und die dort genannten Kriterien zu berücksichtigen. Neben der Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a)) umfasst das nach Art. 32 Abs. 1 lit. b) insbesondere die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Von der Geeignetheit im Sinne der Vorschrift ist zunächst einmal auszugehen, wenn diese Ziele gefördert werden.[120] 58

Es ist dabei grundsätzlich begrüßenswert, das **Nutzungsprotokoll** als Speicherort für die einzelnen Datenzugriffe fälschungs- und manipulationssicher gestalten zu wollen. Die Praktikabilität der Vorschläge für die Gewährleistung der Integrität divergiert allerdings. Während die bereits erläuterten *Software Guard Extensions* (SGX) mittels kryptografischer Verfahren in der Theorie eine abgeschottete Umgebung in Prozessoren schaffen, erscheint vor diesem Hintergrund die Notwendigkeit einer – datenschutzrechtlich ohnehin streitbaren[121] - Blockchain-Lösung als nicht notwendig. Da aber auch die Anwendung der *Software SGX* offensichtlich zu einem regelmäßigen Auftreten von Sicherheitslücken geführt hat,[122] ist der Einsatz vergleichbarer Software zu empfehlen und daher zu evaluieren. 59

3. Rechte der betroffenen Personen

Neben den bereits dargestellten Informationsrechten und Auskunftspflichten nach Art. 12 ff. DSGVO als Ausprägungen des Transparenzgrundsatzes ist darauf zu achten, dass auch die **Rechte der Betroffenen** nach den Art. 16 ff. DSGVO umgesetzt werden. Der Verantwortliche muss dazu gem. Art. 12 Abs. 1 S. 1 DSGVO einerseits geeignete Maßnahmen treffen, um die dafür notwendigen Informationen in transparenter Weise zur Verfügung zu stellen. Andererseits muss er den betroffenen Personen gem. Art. 12 Abs. 2 S. 1 DSGVO aber auch die Ausübung der Rechte nach den Art. 15-22 DSGVO erleichtern. Zur Umsetzung der Erleichterung bzw. Unterstützung in der Praxis kommen 60

---

[118] *Heberlein* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, DSGVO Art. 5 Rn. 28.
[119] *Frenzel* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, DSGVO Art. 5 Rn. 46 ff.
[120] *Jandt* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, DSGVO Art. 32 Rn. 5.
[121] Zur Blockchain-Problematik vor dem Hintergrund des Rechts auf Vergessenwerden s. auch *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251.
[122] Vgl. https://www.heise.de/news/UHD-Blu-rays-lassen-sich-nicht-mehr-auf-neuen-PCs-wiedergeben-SGX-deaktiviert-6326346.html.

verschiedene Handlungsformen in Betracht, darunter die klare Definition von Zuständigkeiten und Ansprechpartnern (Verantwortlicher, Stellvertreter, Datenschutzbeauftragter) sowie der innerorganisatorischen Weiterleitung von Anträgen[123], die Einrichtung von elektronischen Kontaktformularen[124], die bereits anfänglich in Betracht gezogenen Schnittstellen und Formate für Anträge nach Art. 20 DSGVO[125], ein Löschkonzept (ggfs. nach Umsetzung von DIN Norm 66398).[126]

61 Diese bereits in der DSGVO enthaltenen und umzusetzenden Rechte decken sich auch mit den **Ergebnissen des Praxislaboratoriums** im Hinblick auf Workshop und Umfrage zum Use Case der Skilldatenbank und der Expertensuche. Ausgangspunkt des Use Cases ist wiederum *iTrac* (auf Basis von *Jira*). Das Tool macht sichtbar, woran die Beschäftigten gerade arbeiten, wie der Arbeitsstand ist und an welcher Stelle Probleme auftauchen. Dabei werden Arbeitsschritte dokumentiert und der Entwicklungsprozess kann dokumentiert werden. Dabei werden Aufgaben an Personen durch „Tickets" zugewiesen, die dann bearbeitet und nach Abschluss geschlossen werden können. Die Expertensuche ermöglicht es den Mitarbeitenden und Führungskräften, Personen zu finden, die zu bestimmten Themenbereichen bereits Tickets bearbeitet oder abgeschlossen haben, sodass sie schnell Experten innerhalb des Konzerns auffinden können. Auf die Frage, warum Mitarbeitende das Tool nicht nutzen würden, gaben einige an, dass dadurch verzerrte Rückschlüsse über tatsächliche Skills getroffen werden könnten. Es könnte zu Fehlinterpretationen kommen, die Aussagekraft fehle, wenn z.B. Soft-Skills nicht berücksichtigt werden oder historische Daten fehlen. Auf die Frage, was bei einer Umsetzung berücksichtigt werden sollte, wurden das Recht auf Löschung und Korrektur der Daten genannt, eine Schlichtungsstelle für strittige Daten sowie jederzeitige Abfragemöglichkeiten über die gespeicherten Daten sowie die Zugriffe, um ein verzerrtes Bild zu vermeiden und die Kontrolle zu haben. Hier würden sich ebenfalls besondere Probleme im Hinblick auf die Erforderlichkeit der Blockchain zeigen, da das Recht auf Löschung der Daten in der Blockchain nur möglich ist, wenn die Mehrheit der User dieser Löschung zustimmt. Ob sich eine Anonymisierung durch Löschung der Daten aus der Blockchain insbesondere im Zuge mit Big Data überhaupt realisieren lässt, erscheint ebenso fraglich.[127]

4. Data Protection by design und Transparency by design

62 Die Pflichten des Verantwortlichen zu **datenschutzfreundlichen Voreinstellungen** und **Datenschutz durch Technikgestaltung** ergeben sich aus Art. 25 Abs. 1 und 2 DSGVO.

---

[123] *Franck* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 12 Rn. 13.
[124] *Franck* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 12 Rn. 15 mit Hinweis auf EG 59.
[125] *Franck* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 12 Rn. 15.
[126] *Franck* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 12 Rn. 15.
[127] Vgl. so u.a. auch *Hofmann/Johannes*, DSGVO: Anleitung zur autonomen Auslegung des Personenbezugs, ZD 2017, S. 221, 225.

Diese – oft auch ungenau unter privacy by design und privacy by default bezeichneten Pflichten[128] - gehen in ihrer Konzeption und Diskussion bereits bis in die 1990er Jahre zurück und vereinen den Gedanken, Datenschutz bereits bereits in der Konzeption zu implementieren.[129] Als „Kernelement[e] und Innovationsbaustein[en]"[130] wurden sie in der DSGVO letztlich als bußgeldbewehrte Pflicht der Verantwortlichen eingeführt, um den Datenschutz möglichst frühzeitig mit einzubinden und komplexe Anpassungen erstmal entwickelter Produkte zu vermeiden.[131] Zu beachten ist hierbei, dass sich die Verpflichtung nicht direkt an die Hersteller oder Programmierer richtet, sondern an den Verantwortlichen nach der DSGVO.[132] Fallen Verantwortlicher und Hersteller in einer Person oder Stelle zusammen, treffen diese jedoch auch die maßgeblichen Pflichten.[133] Die Hersteller sollen ermutigt werden[134], die Grundsätze zu berücksichtigen, sodass indirekt eine positive Wirkung am Markt erzielt wird.[135] Die Norm konkretisiert die Datenschutzgrundsätze des Art. 5 DSGVO[136]. Dabei wird zwar exemplarisch die Datenminimierung genannt, sodass data protection by design auch als besondere Ausprägung des Grundsatzes der Datenminimierung angesehen wird, allerdings differenziert Art. 25 Abs. 1 DSGVO nicht bei den Grundsätzen und nennt alleine die Umsetzung der Datenschutzgrundsätze. Unter diesen Voraussetzungen kann die Fortentwicklung der Transparenz durch transparency by design[137] auch als innovative Umsetzung des datenschutzrechtlichen Grundsatzes der Transparenz durch data protection by design eingeordnet werden. Dennoch ist auch hier zu beachten, dass eine rechtswidrige Datenverarbeitung durch die Herstellung der Transparenz nicht rechtmäßig gemacht werden kann. Dies gilt auch, wenn der Grundsatz der Transparenz bereits durch Technikgestaltung in der Konzeption umgesetzt wird.

5. Rechtmäßigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten des **Arbeitnehmers durch den Arbeitgeber** bedarf aufgrund der beschriebenen Machtasymmetrien und deren Einfluss auf eine freiwillige Einwilligung zur Rechtmäßigkeit bestenfalls einer vertraglichen oder gesetzlichen (wie im Falle der Leistungskontrolle) Grundlage. Die auf dem Konzept der **63**

[128] In der englischen Version der DSGVO (GDPR) wird stattdessen von data protection by design/default gesprochen; vgl. dazu Hartung in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO Art. 25 Rn. 1.

[129] Nolte/Werkmeister in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 25 Rn. 1.

[130] *Martini* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, DSGVO Art. 25 Rn. 8.

[131] Dazu auch *Nolte/Werkmeister* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 25 Rn. 2 mwN.

[132] *Nolte/Werkmeister* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 25 Rn. 11.

[133] *Nolte/Werkmeister* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 25 Rn. 11.

[134] Erwägungsgrund 78 S. 4 der DSGVO.

[135] Vgl. dazu Erwägungsgrund 78 S. 4 der DSGVO; *Lang* in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, DSGVO Art. 25 Rn. 27.

[136] *Martini* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, DSGVO Art. 25 Rn. 2; *Nolte/Werkmeister* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 25 Rn. 8.

[137] Vgl. dazu umfassend Zieglmeier/Pretschner, Trustworthy Transparency by Design, S. 1.

Inversen Transparenz entwickelte Toolchain hingegen sorgt selbst auch für eine umgekehrte, „inverse“ Datenverarbeitung im Verhältnis Arbeitnehmer – Arbeitgeber, indem auch der Arbeitnehmer (der in der Regel das Datensubjekt darstellt) durch die Ausgabe auf die Zugriffe durch den Arbeitgeber oder Vorgesetzten (die in der Regel auf die Daten im Anwendungsfall zugreifen). Die Anforderungen an die Rechtmäßigkeit dieser Verarbeitung sollen nun im Folgenden erörtert werden.

a) Anwendungsbereich – Verarbeitung personenbezogener Daten

64 Mittelpunkt des Konzepts der Inversen Transparenz Toolchain ist es gerade, im Sinne der **Datennutzungstransparenz,** auf Daten zugreifende Systemteilnehmer zu identifizieren. Da der Zugriff der zugreifenden Person – das ist nach dem Zweck des Konzepts in der Regel der Arbeitgeber bzw. Vorgesetzte - zuzuordnen ist, handelt es sich wie bereits dargestellt um die Verarbeitung (Art. 4 Nr. 2 DSGVO) personenbezogener Daten (Art. 4 Nr. 1 DSGVO) im Sinne des Art. 2 Abs. 1 DSGVO, sodass der sachliche Anwendungsbereich der DSGVO unproblematisch eröffnet ist.

b) Rechtmäßigkeit der Datenverarbeitung

Ob diese Datenverarbeitung im **Einzelfall** rechtmäßig ist, ist stark von den konkreten Umständen des Einzelfalles abhängig und kann nicht pauschal für die generelle Anwendung der Toolchain klassifiziert werden.

(aa) Keine Anwendbarkeit des § 26 BDSG

65 Die für die über die Öffnungsklausel des Art. 88 Abs. 1 DSGVO grundsätzlich im Beschäftigungskontext maßgebliche nationale Regelung des § 26 BDSG ist für den inversen Fall, dass Arbeitnehmer personenbezogene Daten von Arbeitgebern verarbeiten, nicht anwendbar. Dieser gilt nur für die Verarbeitung von **Beschäftigtendaten**, d.h. gem. § 26 Abs. 8 BDSG insbesondere für Daten von Arbeitnehmern als vertraglich zu weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit Verpflichtete[138] bzw. auch leitenden Angestellte in größeren hierarchischen Organisationsstrukturen.[139] Ausgehend hiervon stellt sich auf den ersten Blick automatisch die Frage, ob § 26 BDSG dann „immerhin“ anwendbar ist, wenn Arbeitnehmer mittels der Toolchain auf Zugriffsdaten leitender Angestellter zugreifen. Neben dem Beschäftigtenbegriff spricht aber auch der intendierte Schutzzweck von Art. 88 DSGVO und § 26 BDSG gegen ein solches Verständnis im umgekehrten Verhältnis. Diese Vorschriften berücksichtigen nämlich gerade den erhöhten Schutzbedarf von Arbeitnehmern im von strukturell bedingten Machtasymmetrien und Abhängigkeiten

---

[138] *Gola* in Gola/Heckmann, BDSG, 13. Aufl. 2019, § 26 BDSG Rn. 14.
[139] *Riesenhuber* in Wolff/Brink, BeckOK Datenschutzrecht, 38. Edition, BDSG § 26 Rn. 22; BAG, Beschluss v. 9.4.2019 – 1 ABR 51/17, Auskunftsanspruch des Betriebsrats über (sensible) personenbezogene Arbeitnehmerdaten, NZA 2019, S. 1055 Rn. 34.

geprägten Beschäftigungsverhältnis.[140] In Betracht kommt eine Anwendung dagegen für den Fall, dass Arbeitgeber die Zugriffe der Arbeitnehmer einsehen. Denn durch die Einführung der Inversen Transparenz werden nicht nur neue Datenzugriffsmöglichkeiten für die Arbeitnehmer eingeführt. Wechselseitig haben auch die Arbeitgeber die Möglichkeit, abzufragen, wer welche Daten über sie eingesehen hat. Diese neue Datenverarbeitung ist zu trennen von der Frage, inwieweit die Ursprungsdaten (*Jira*/ *iTrac* oder anderer Softwaretools) rechtmäßig sind, sondern welche Ergebnisse sich aus der Implementierung der Toolchain ergeben. In diesem Fall ist auf Einhaltung der beschriebenen Grundsätze zum Arbeitnehmerdatenschutz und zur Leistungskontrolle, zu achten. Der Fokus der Darstellung soll hier aber auf dem innovativen Verhältnis zwischen Arbeitnehmeranfragen über die Arbeitgeberzugriffe liegen.

Zweck der inversen Transparenz ist vor allem, dem durch diese strukturelle Machtasymmetrie erzeugten Misstrauen von Arbeitnehmern gegenüber der Verwendung der über sie durch Arbeitgeber erhobenen Datenmengen zu begegnen. Statt einer Verarbeitung „von oben nach unten" ist die Bereitstellung des Datenzugriffs vielmehr auch eine Verarbeitung „von unten nach oben", auf die § 26 BDSG nicht anwendbar ist. **66**

(bb) Art. 6 Abs. 1 DSGVO

Ist ein Sachverhalt wie vorliegend innerhalb einer Öffnungsklausel nicht abschließend geklärt, gelten die Regelungen der DSGVO weiter **unmittelbar**,[141] sodass maßgebliche Vorschrift für die Rechtmäßigkeit der „inversen Verarbeitung" Art. 6 Abs. 1 DSGVO ist. Die potenziellen Rechtfertigungsgründe sollen dabei im Kontext der inversen Transparenz genauer betrachtet werden. **67**

(1) Einwilligung, Art. 6 Abs. 1 lit. a) DSGVO

Als freiwilliger Rechtfertigungstatbestand für den Zugriff durch die Datensubjekte kommt zunächst nach Art. 6 Abs. 1 lit. a) DSGVO die Einwilligung des Zugreifenden in Betracht. Eine wirksame **Einwilligung** liegt im Sinne des Art. 4 Nr. 11 DSGVO bei jeder freiwillig für den bestimmten Fall, in informierter Weise und unmissverständliche abgegeben Willensbekundung hinsichtlich der Verarbeitung personenbezogener Daten. Da eine Interessensabwägung oftmals nur aufgrund der Einzelfallumstände knapp ausfällt, ist die Einwilligung für die Rechtfertigung von Datenverarbeitungen die rechtssichere Wahl.[142] **68**

Formell erfordert die Einwilligung vor allem die **Einsichtsfähigkeit** der betroffenen Person,[143] eine bestimmte Form muss die Einwilligung allerdings nicht aufweisen. Materiell steht im Zentrum der Einwilligung das Prinzip der **Freiwilligkeit**, das sich **69**

---

[140] *Braun* in Heckmann/Paschke, jurisPK-Internetrecht, Kap. 7 Rn. 11; *Gräber/Nolden* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, BDSG § 26 Rn. 4.
[141] Vgl. *Selmayr/ Ehmann* in Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Einführung Rn. 88.
[142] Taeger in Taeger/Gabel, DSGVO-BDSG-TTDSG, DSGVO Art. 6 Rn. 30.
[143] *Tinnefeld/Conrad*, Die selbstbestimmte Einwilligung im europäischen Recht, ZD 2018, S. 391, 393.

wiederum in Freiheit von Zwang und Wahlfreiheit sowie Informiertheit unterteilen lässt.[144] Im Rahmen der **Wahlfreiheit** sind vor allem auch strukturelle Machtasymmetrien zulasten des Einwilligenden berücksichtigen.[145] Eine Wahlfreiheit ist zudem nicht anzunehmen, wenn zu diversen Verarbeitungen lediglich die Möglichkeit einer pauschalen Einwilligungserklärung besteht, obwohl die Gelegenheit zur Einwilligung im Einzelfall angezeigt wäre.[146] Pauschaleinwilligungen erfüllen daher nicht die Anforderungen an eine wirksame Einwilligung.[147] **Informiertheit** bedeutet, dass dem Einwilligenden Umfang und Tragweite seiner Einwilligung bewusst sein müssen.[148] Schließlich muss nach dem Grundsatz der **bestimmten Einwilligung** dem Betroffenen erkennbar sein, welche Daten zu welchem Zweck verarbeitet werden sollen.[149]

70 Angewandt auf den Fall der inversen Transparenz lässt sich konstatieren, dass eine pauschale Aussage über die Einwilligung von Arbeitgebern bzw. Führungskräften nicht getroffen werden kann. **Einwilligungssubjekt** im Rahmen der Verarbeitung Arbeitnehmer – Arbeitgeber ist der Arbeitgeber, dessen Datenzugriff durch die Ausgabe dem Arbeitnehmer zur Verfügung gestellt werden soll. Die angesprochene **Machtasymmetrie** wirkt sich in diesem „umgekehrten" Verhältnis nicht negativ auf die Wahlfreiheit aus. Und auch die weiteren Parameter der Freiwilligkeit, der Informiertheit und der Bestimmtheit der Einwilligung dürften grundsätzlich bei Anwendung der Toolchain nicht scheitern, da das Empowerment als gesamtbetriebliches Ziel ja gerade von einer vertrauten Umgebung zwischen Arbeitnehmern und Arbeitgebern im Hinblick auf die Funktion des sichtbaren Datenzugriffes ausgeht.

71 Die entscheidende Frage und der Grund dafür, die Frage nach der Rechtmäßigkeit durch Einwilligung nicht pauschal beantworten zu können ist letztlich aber eine andere, nämlich ob ein **Arbeitgeber** bzw. eine Führungskraft im Rahmen inverser Transparenz überhaupt in die Erfassung ihrer Zugriffe durch die Toolchain einwilligen wird. Dies erfordert für eine pauschale Aussage weiteren **Forschungsbedarf** und ist daher im Einzelfall zu betrachten. Da die Einwilligung somit nicht für eine generelle Einordnung der Rechtmäßigkeit der Verarbeitung durch die Toolchain herangezogen werden kann (sondern nur im Einzelfall), sollen nun die gesetzlichen Rechtfertigungstatbestände auf die Verarbeitung in der Toolchain herangezogen werden.

---

[144] So auch *Heckmann/Paschke* in Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, DSGVO Art. 7 Rn. 48.
[145] Vgl. auch *Heckmann/Paschke* in Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, DSGVO Art. 7 Rn. 53.
[146] Erwägungsgrund 43 zur DSGVO, S. 2.
[147] *Schulz* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 7 Rn. 34..
[148] Vgl. auch *Heckmann/Paschke* in Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, DSGVO Art. 7 Rn. 57.
[149] *Heckmann/Scheurer* in Heckmann/Paschke, jurisPK-Internetrecht, 7. Aufl. 2021, Kap. 9 Rn. 331 mwN.

(2) Erforderlichkeit zur Erfüllung eines Vertrages, Art. 6 Abs. 1 lit. b) DSGVO

Nach Art. 6 Abs. 1 lit. b) DSGVO kann eine Datenverarbeitung auch dann rechtmäßig sein, wenn sie zur **Erfüllung eines Vertrages** erforderlich ist. Zu fragen ist daher, ob die Ausgabe des Datenzugriffs für das Datensubjekt zur Erfüllung des Arbeitsvertrages erforderlich ist. **Erforderlich** ist eine Datenverarbeitung in diesem Sinne dann, wenn sie für die Erfüllung des Vertrages (oder die Durchführung vorvertraglicher Maßnahmen) **notwendig** ist,[150] was bereits die Sinnhaftigkeit zur Effizienzsteigerung und Kostenminimierung miteinschließt.[151] Es ist aber vorauszusetzen, dass die Verarbeitung **für die Erfüllung der konkreten Vertragszwecke** notwendig und nicht nur nützlich ist, wobei in der Norm nicht zwischen Haupt- und Nebenpflichten differenziert wird.[152] Auch wenn durch die Inverse Transparenz ein Empowerment gestärkt und Misstrauen abgebaut wird, ist die Stufe der Notwendigkeit zur **Erfüllung** arbeitsvertraglicher Pflichten wohl nicht erreicht. 72

(3) Rechtliche Verpflichtung 73

Die **Erfüllung einer rechtlichen Verpflichtung** könnte die Verarbeitung des Datenzugriffs nach Art. 6 Abs. 1 lit. c) DSGVO ebenfalls rechtmäßig gestalten. „Rechtliche Verpflichtung" in diesem Sinne meint grundsätzlich eine gesetzliche Verpflichtung aus Rechtsvorschriften, aufgrund derer Daten verarbeitet werden dürfen.[153] Eine solche ist für das Konzept der inversen Transparenz grundsätzlich nicht ersichtlich, wobei ein Regulierungsbedürfnis de lege ferenda in jedem Fall weitere Forschung notwendig macht.

Im privatwirtschaftlichen Kontext können allerdings auch **Tarifverträge** und **Betriebsvereinbarungen** eine derartige rechtliche Verpflichtung auslösen, da diese über § 4 Abs. 1 TVG und § 77 Abs. 4 S. 1 BetrVG normative Außenwirkung erlangen.[154] Nach § 88 BetrVG können Arbeitgeber und Betriebsrat auch außerhalb der verpflichtenden Mitbestimmung des Betriebsrates freiwillige Vereinbarungen schließen. Grundsätzlich haben die Arbeitnehmer-Tarifpartei und der Betriebsrat bei Schaffung von Kollektivvereinbarungen in Abwägung mit den Arbeitgeberinteressen die **Persönlichkeitsrechte der Arbeitnehmer** zu beachten.[155] Dies basiert auf § 75 Abs. 2 BetrVG, wonach Arbeitgeber und Betriebsrat die Persönlichkeitsrechte der Arbeitnehmer zu schützen haben. Gegenstand von **Betriebsvereinbarungen** können sowohl Regelungen zugunsten als auch zulasten des Arbeitnehmers sein.[156] Auch im Rahmen 74

---

[150] So auch *Schulz* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 6 Rn. 38.
[151] Vgl. auch *Taeger* in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 6 DSGVO Rn. 84.
[152] So u.a. auch *Heberlein* in in Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, DSGVO Art. 6 Rn. 13.
[153] *Buchner/Petri* in Kühling/Buchner, DSGVO BDSG, 2. Aufl. 2018, DSGVO Art. 6 Rn. 76.
[154] Vgl. auch *Taeger* in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 6 DSGVO Rn. 84.
[155] *Taeger* in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 6 DSGVO Rn. 87.
[156] *Werner* in Beck'scher Online Kommentar Arbeitsrecht, 62. Edition, BetrVG § 77 Rn. 37.

freiwilliger Betriebsvereinbarungen finden diese ihre Grenze aber in § 75 BetrVG und damit über § 75 Abs. 2 BetrVG auch in der informationellen Selbstbestimmung der Arbeitnehmer.[157]

75 Auf Basis einer **Betriebsvereinbarung** könnte im Grundsatz daher eine rechtliche Verpflichtung im Sinne des Art. 6 Abs. 1 lit. c) DSGVO geschaffen werden. Der Betriebsrat kann, soll und wird in der Regel darauf hinwirken, dass im Rahmen derartiger Betriebsvereinbarungen auf (unzulässige) Leistungskontrollen zulasten der Arbeitnehmer verzichtet wird.[158] Dabei muss im Übrigen aber die informationelle Selbstbestimmung der Arbeitnehmer gewahrt werden. Ob dies im Rahmen des Einsatzes der Toolchain der Fall ist, ist an den in dieser Stellungnahme erörterten Maßstäben zu messen. Schließlich müssten auch Arbeitgeber und Führungskräfte bereit sein, derartige Betriebsvereinbarungen abzuschließen. Dies vermag hinsichtlich einer generellen Bereitschaft – wie bereits im Rahmen der Einwilligung erörtert – nicht abschließend beurteilt werden zu können und muss daher im Einzelfall erörtert werden.

(4) Interessensabwägung

76 Zuletzt kommt die Rechtfertigung nach einem der in der DSGVO zentralen Tatbestände[159], der **Interessensabwägung** gem. Art. 6 Abs. 1 lit f) DSGVO, in Betracht. Danach ist die Verarbeitung rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen und Rechte der betroffenen Person überwiegen. Daraus ergeben sich drei wesentliche Prüfungsschritte.[160] Notwendig ist einerseits das Vorliegen von berechtigten Interessen des Verantwortlichen (1), zur Wahrung derer die Datenverarbeitung erforderlich ist (2). Dagegen stehen in einer Abwägung die Interessen und Grundrechte der betroffenen Personen (3), wobei hier kein „berechtigtes" Interesse, sondern nur ein Interesse gefordert wird. Eine Legaldefinition des berechtigten Interesses besteht nicht, wobei hier nicht nur rechtliche Interessen, sondern auch konkretisierte „tatsächliche, wirtschaftliche oder ideelle Interessen"[161] erfasst sind. Die Erforderlichkeit richtet sich insbesondere nach den Datenschutzgrundsätzen, sodass u.a. zu prüfen ist, ob die Verarbeitungen zur Erreichung des Zwecks erforderlich sind (s.o.).[162] Demgegenüber dürfen keine Interessen[163] der betroffenen Personen entgegenstehen. In der Abwägung ist nach

---

[157] *Werner* in Beck'scher Online Kommentar Arbeitsrecht, 62. Edition, BetrVG § 77 Rn. 41.
[158] Diese Vereinbarung wurde beispielhaft auch beim Einsatz von *iTrac* und *Jira* bei der Projektpartnerin der Software AG ausgeschlossen.
[159] *Albers/Beit* in Wolff/Brink, BeckOK Datenschutzrecht, 39. Edition, DSGVO Art. 6 Rn. 63.
[160] Vgl. dazu auch *Frenzel* in Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, DSGVO Rn. 27f.; *Buchner/Petri* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO Art. 6 Rn. 146ff.
[161] *Buchner/Petri* in Kühling/Buchner, DSGVO BDSG, 3. Aufl. 2020, DSGVO Art. 6 Rn. 146a; so auch *Schulz* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 6 Rn. 57.
[162] *Schulz* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 6 Rn. 57.
[163] Hier sind keine „berechtigten Interessen" erforderlich, sondern lediglich interessen.

Erwägungsgrund 47 S. 2, 3 ist die Beziehung des Verantwortlichen und der betroffenen Person zu berücksichtigen (z.B. Kunden, aber auch im Dienst stehende Personen) sowie die Frage, inwieweit die betroffene Person angesichts der jeweiligen Umstände, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für den entsprechenden Zweck erfolgen wird. So ist in einem Gesamtkontext auch auf den Erwartungshorizont in der jeweiligen Situation abzustellen. Zu beachten ist, dass im Verhältnis von Arbeitgeber (bzw. Führungskräften) zu Arbeitnehmer eine Rechtfertigung insbesondere dann in Betracht kommt, wenn es sich um „beschäftigungsfremde Zwecke“[164] handelt, da davon nur solche Verarbeitungen gefasst werden können, die nicht bereits durch die Erfüllung des Vertrags erfasst sind.[165]

Im Fall von Inverser Transparenz gilt es die **gegenseitigen Interessen** darzustellen. Zum einen soll dadurch das Innovationspotential ungenutzter Daten gestärkt werden, um Arbeitsprozesse zu optimieren, eine digitale und vernetzte Arbeitswelt zu schaffen und Wertschöpfung aus den zur Verfügung stehenden Informationen zu ziehen. Demgegenüber ist zu berücksichtigen, dass die Arbeitnehmer in einem Abhängigkeitsverhältnis zum Arbeitgeber stehen und die Macht- sowie Informationsasymmetrie nicht eigenständig ausgleichen können. Hier ist der Schutz vor ungerechtfertigten oder erhöhten Leistungskontrollen zu berücksichtigen. Gleichwohl zeigen die Ergebnisse der Umfrage im Praxisworkshop zur Expertensuche, dass eine Einführung des Tools nach Einschätzung der Teilnehmenden dazu führen könnte, dass Druck entsteht, sich bestimmte Skills anzueignen oder Konkurrenzgedanken („Jeder gegen Jeden“) aufkommen. Insgesamt bleibt in weiterer Forschung zu ermitteln, inwieweit die „Demokratisierung“[166] der Daten durch Inverse Transparenz zu einer Angleichung der wechselseitigen Interessen führen kann, indem das Vertrauen gestärkt wird und die Datennutzung ggfs. sogar im beiderseitigen Interesse – zur Verbesserung der eigenen Arbeitsleistung sowie zur erhöhten Wertschöpfung – erhöht wird. Die Interessensabwägung betrifft naturgemäß die Abwägung der widerstreitenden Interessen im Einzelfall und nicht generell. Die eben erörterten und aus den Ergebnissen des Projekts resultierenden Parameter sollen aber indiziell im Einzelfall in die Abwägung eingestellt werden. 77

[164] *Gola* in Gola, DSGVO, 2. Aufl. 2018, DSGVO Art. 6 Rn. 102.

[165] *Gola* in Gola, DSGVO, 2.Aufl. 2018, DSGVO Art. 6 Rn. 102.

[166] *Hess/Neuburger/Gierlich-Joas*, Forschungsreport Inverse Transparenz, S. 39.

C. Zusammenfassung und Handlungsempfehlungen

Schließlich soll eine Zusammenfassung der wichtigsten Aspekte der Stellungnahme im Hinblick auf die Inverse Transparenz Toolchain erfolgen und – wo möglich – Handlungsempfehlungen für die künftige Nutzung formuliert werden. Wichtig ist dabei klarzustellen, dass eine pauschale und abschließende datenschutzrechtliche Bewertung der Toolchain hinsichtlich ihrer Rechtmäßigkeit aus den genannten Gründen nicht erfolgen kann. Dies ist anhand der einzelfallbezogenen Anwendung der Toolchain im Konzept der Inversen Transparenz zu beurteilen. Die in der Stellungnahme ausgeführten Überlegungen können dabei in diese Einzelfallbetrachtung eingestellt werden.

Abschließend lassen sich folgende Aspekte und Handlungsempfehlungen identifizieren:

- Der hinter der Inversen Transparenz Toolchain stehende Grundsatz der *Transparency by Design* ist eine grundsätzlich geeignete Konkretisierung des aus Art. 25 Abs. 1 DSGVO folgenden Grundsatzes der *data protection by design*, da mit dem Grundsatz der Transparenz nach Art. 5 Abs. 1 lit. a) Var. 3 DSGVO bereits ein tragender Grundsatz der DSGVO im Softwaredesign mitgedacht wird und die informationelle Selbstbestimmung von Mitarbeitenden gestärkt werden kann.

- Vor dem Hintergrund des datenschutzrechtlichen *Grundsatzes der Transparenz* aus Art. 5 Abs. 1 lit. a) Var. 3 DSGVO ist das Konzept der Inversen Transparenz hinsichtlich des Ziels der Vermeidung heimlicher und unbekannter Datenverarbeitungen generell positiv zu bewerten. Die wechselseitige Transparenz und die aktive, gleichstufige Einbeziehung von Führungskräften und Mitarbeitenden in den Informationsfluss kann heimliche Datenverarbeitungen und potenziellen Datenmissbrauch mit dem „Watch the Watcher"-Prinzip sichtbar machen. Dies könnte das Bewusstsein über verarbeitete Daten stärken und so die selbstbestimmte Ausübung der informationellen Selbstbestimmung stärken.

- Dabei ist zu berücksichtigen, dass eine *ohnehin rechtswidrige Verarbeitung* personenbezogener Daten durch erhöhte (inverse bzw. allgemeine) Transparenz *nicht automatisch rechtmäßig* wird. Ansonsten könnte nämlich die Gefahr entstehen, dass Transparenz als Rechtfertigung für immer weitere Datenverarbeitungen herangezogen wird und sich somit kontraproduktiv auf das Konzept der Inversen Transparenz einwirken. Das Risiko der Zementierung bestehender struktureller Machtasymmetrien sowie unzulässiger Leistungskontrollen wäre bei einer steigenden Verarbeitung personenbezogener Daten inhärent.

- Sofern eine (Leistungs- oder Verhaltens-)Kontrolle oder ein Zugriff auf personenbezogene Daten eines Mitarbeitenden durch eine Führungskraft aber auf

eine rechtliche Grundlage gestützt werden kann, ist vor dem Hintergrund des *Grundsatzes der Datenminimierung* gemäß Art. 5 Abs. 1 lit. c) DSGVO zu erörtern, ob es grundsätzlich der Implementierung der Inversen Transparenz Toolchain und weiteren Datenverarbeitungen überhaupt bedarf. Diese verfolgt mit der Nutzung bislang ungenutzter Datenpotenziale aber einen anderen Zweck, nämlich die Stärkung des Empowerments und der informationellen Selbstbestimmung von Mitarbeitenden. Ob dieser Zweck letztlich wirklich erreicht werden kann ist eine soziologische und arbeitsethische Fragestellung, die weiterer Forschung bedarf.

- Im Hinblick auf die sog. *Umgebungsnutzung von Daten (ambient usage)* und unnötig ausgelöste Datenzugriffe in der Toolchain ist im Sinne der Datensparsamkeit und des bewussten Umgangs mit Daten technisch unbedingt die modifizierte Lösung einer Protokollierung nur auf explizite Anfrage zu empfehlen.

- Eine mittels kryptographischer Verfahren gesicherte (Prozessor-)Umgebung zur (fälschungssicheren) Speicherung der Datenzugriffe im Nutzungsprotokoll und damit eine der angesprochenen – jedoch Sicherheitslücken aufweisenden – Software vergleichbare Lösung ist im Sinne der *Vertraulichkeit und* Integrität nach Art. 5 Abs. 1 lit. f) DSGVO geboten. Die Notwendigkeit einer Blockchain-Lösung ist gerade im Hinblick auf das Recht auf Löschung und die Datenminimierung zweifelhaft und daher nicht zu empfehlen.

- Schließlich muss auch die durch das Konzept der Inversen Transparenz und durch die Toolchain in den Mittelpunkt gerückte *Datenverarbeitung* personenbezogener Daten des Zugreifenden (i.d.R. Führungskraft) durch das Datensubjekt (i.d.R. Mitarbeitende) datenschutzrechtlich *gerechtfertigt* sein. Die Rechtmäßigkeit bestimmt sich in diesem Verhältnis maßgeblich nach Art. 6 Abs. 1 DSGVO und nicht nach § 26 BDSG. Dabei kann sie nicht pauschal, sondern muss vielmehr für den Einzelfall betrachtet werden. Für eine Einwilligung bzw. Betriebsvereinbarung als rechtliche Verpflichtung müssen Führungskräfte im konkreten Fall hierzu bereit sein. Im Rahmen einer Interessensabwägung können die Ansätze dieser Stellungnahme zu berücksichtigen sein.