A. Arbeitnehmerkontrollen

Abschnitt 1 – Perspektive Arbeitgeber

I. Einleitung

Arbeitgeber haben vielerlei legitime Gründe dafür, ihre Mitarbeiter zu kontrollieren. Im Vordergrund steht dabei die Kontrolle der Arbeitsleistung, der Schutz von im Betrieb erwirtschafteten Ergebnissen und vom Arbeitgeber bereitgestellten Sachmitteln sowie die Einhaltung sonstiger betrieblicher Vorgaben im weiteren Sinne. Studien gehen davon aus, dass deutsche Unternehmen allein durch Straftaten eigener Mitarbeiter jährlich Einbußen von 2,5 bis 17,5 Milliarden EUR erleiden.[1] Dies und nicht zuletzt die technischen Entwicklungen des letzten Jahrzehnts, die den mit Kontroll- und Überwachungsmaßnahmen einhergehenden Aufwand für den Arbeitgeber immer geringer werden ließen, machen Fragen der Mitarbeiterkontrolle zu einem aktuellen und viel diskutierten Thema. Kern der Diskussion ist stets die Auflösung des Spannungsverhältnisses zwischen dem arbeitgeberseitigen Kontrollinteresse und dem Allgemeinen Persönlichkeitsrecht der Mitarbeiter. Zahlreiche medienwirksame Skandale bei bekannten Konzernen in der Vergangenheit haben gezeigt, dass dabei dem Persönlichkeitsrecht der Mitarbeiter nicht immer hinreichende Bedeutung beigemessen wird.[2] Die Durchführung von Mitarbeiterkontrollen wirft daher spezielle individual- und kollektivarbeitsrechtliche sowie datenschutzrechtliche Fragestellungen auf. **1**

In diesem Beitrag soll nach einer Darstellung der rechtlichen Grundlagen und Grenzen von Mitarbeiterkontrollen auf ausgewählte Formen der Kontrollen, insbesondere auf Spind- und Taschenkontrollen sowie auf die im Zuge der technischen Weiterentwicklung verstärkt aufgekommene Diskussion der Videoüberwachung eingegangen werden. Zudem werden auch die für Unternehmen praxisrelevanten Kontrollmaßnahmen der E-Mail- und Telefonüberwachung beleuchtet. Erörterungen zu den Folgen unzulässiger Mitarbeiterkontrollen seitens des Arbeitgebers schließen den Beitrag ab. **2**

---

1 *Byers*, Mitarbeiterkontrollen, Rn. 132; Sonderauswertung des Gesamtverbandes der Deutschen Versicherungswirtschaft, https://www.gdv.de/de/medien/aktuell/versicherer-warnen-vor-hohen-schaeden-durch–kriminelle-mitarbeiter-50522 (zuletzt abgerufen: 1.3.2022).

2 BT-Drs. 16/13657, 20; Beispiele zu Verfahren wegen Videoüberwachung gegenüber Mitarbeitern, z. B. Bußgeld gegen notebooksbilliger.de: *Kuntz*, ZD-Aktuell 2021, 05025; Bußgeld für H&M: *Caspar*, ZD-Aktuell 2020, 07328.

II. Rechtliche Rahmenbedingungen der Mitarbeiterkontrolle

1. Ausgangspunkt: Allgemeines Persönlichkeitsrecht des Mitarbeiters versus Informationsinteresse des Arbeitgebers

3 Kontrollmaßnahmen stellen sich regelmäßig als Eingriff in das **Allgemeine Persönlichkeitsrecht** der Mitarbeiter aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Je nach Art der Kontrollmaßnahme sind unterschiedliche Ausprägungen des Persönlichkeitsrechts betroffen. So steht eine Videoüberwachung des Mitarbeiters mit dessen Recht am eigenen Bild in Konflikt, während Taschen- und Spindkontrollen die Privatsphäre des Mitarbeiters berühren.[3] Die Überwachung der Kommunikation des Mitarbeiters über vom Arbeitgeber zur Verfügung gestellte Kommunikationsmittel, insbesondere das „Mitlesen" von E-Mails, erweist sich unter dem Gesichtspunkt der informationellen Selbstbestimmung als problematisch.[4]

4 Diesen Eingriffen steht das **Informationsinteresse des Arbeitgebers** gegenüber. Als Gläubiger der vom Mitarbeiter geschuldeten Arbeitsleistung und Inhaber der betrieblichen Sachmittel hat der Arbeitgeber ein berechtigtes Interesse daran, Arbeitsleistung und Verhalten seiner Mitarbeiter zu überwachen, damit er im Hinblick auf Schlechtleistung oder Nebenpflichtverletzungen geeignete Maßnahmen ergreifen und im Falle des Bestreitens ihre Berechtigung gerichtsfest beweisen kann.[5] Darüber hinaus trifft den Arbeitgeber unter dem Stichwort „Compliance" die **Pflicht, rechtswidrige Handlungen seiner Mitarbeiter zu verhindern bzw. aufzudecken** und zu verfolgen.[6] Gleichermaßen hat der Arbeitgeber aber auch darauf zu achten, sich durch unzulässige Kontrollmaßnahmen nicht selbst „incompliant" zu verhalten, da ansonsten zivilrechtliche und ggf. auch strafrechtliche Folgen drohen können.

5 Zum Ausgleich dieser gegenläufigen Interessen bedient sich die Rechtsprechung einer umfassenden **Interessenabwägung**, wobei sie dem Verhältnismäßigkeitsgrundsatz maßgebliche Bedeutung beimisst.[7] Somit können Eingriffe in das Allgemeine Persönlichkeitsrecht gerechtfertigt sein, wenn die konkrete Kontrollmaßnahme geeignet, erforderlich und angemessen ist. Es dürfen keine anderen, zur Befriedigung des Informationsinteresses des Arbeitgebers gleich wirksame und das Persönlichkeitsrecht des Mitarbeiters weniger einschränkende Mittel zur Verfügung stehen. Zudem darf die Schwere des Eingriffs bei einer Ge-

3 BAG, 15.4.2014 – 1 ABR 2/13, NZA 2014, 551, Rn. 43; BAG, 20.6.2013 – 2 AZR 546/12, NZA 2014, 143, Rn. 27.
4 LAG Hessen, 21.9.2018 – 10 Sa 601/18, NZA-RR 2019, 130, Rn. 61.
5 BAG, 29.6.2017 – 2 AZR 597/16, NZA 2017, 1179, Rn. 31.
6 *Thüsing*, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 2 Rn. 1.
7 Vgl. etwa BAG, 29.6.2004 – 1 ABR 21/03, NZA 2004, 1278, 1280; BAG, 25.4.2017 – 1 ABR 46/15, NZA 2017, 1205, Rn. 21.

samtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen. Die Kontrollmaßnahme darf keine übermäßige Belastung für den Mitarbeiter darstellen und muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen. Berücksichtigungswürdige Elemente der Abwägung sind insbesondere die zeitlichen und sachlichen Grenzen der Kontrollen, das Vorhandensein von alternativen Kontrollmaßnahmen, der Kontrollanlass, die Einbindung des Mitarbeiters sowie auch die geplante Verwendung der Ergebnisse.

2. Bedeutung des Datenschutzrechts für die Mitarbeiterkontrolle

Das Kontrollrecht des Arbeitgebers ist ferner durch die datenschutzrechtlichen Vorschriften der DSGVO, des BDSG sowie den spezielleren Vorschriften des TKG und TMG beschränkt. Die Vorschriften des Datenschutzrechts, namentlich die DSGVO und das BDSG, konkretisieren in ihrem Anwendungsbereich den Schutz des Allgemeinen Persönlichkeitsrechts. Ist die Datenverarbeitung nach **datenschutzrechtlichen Maßstäben** zulässig, liegt auch keine Verletzung des Allgemeinen Persönlichkeitsrechts des Mitarbeiters vor.[8] Sofern sich der Eingriff in das Allgemeine Persönlichkeitsrecht des Mitarbeiters durch Verarbeitung personenbezogener Daten vollzieht, bestimmt sich die Zulässigkeit des Eingriffs daher letztlich nach den jeweils einschlägigen datenschutzrechtlichen Vorschriften. **6**

Für die Mitarbeiterkontrolle bedeutet dies, dass es für die Zulässigkeit von Kontrollmaßnahmen entscheidend auf das Datenschutzrecht ankommt. Denn Kontrollmaßnahmen stellen sich nahezu ausnahmslos als Verarbeitung von persönlichen Daten der betroffenen Mitarbeiter dar. Hierbei spielt auch eine Rolle, dass § 26 Abs. 7 BDSG den Anwendungsbereich des Datenschutzrechts im Arbeitsverhältnis auf nichttechnische Formen der Datenverarbeitung ausdehnt. Von § 26 BDSG erfasst ist im Gegensatz zur DSGVO, die grundsätzlich nur für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten Anwendung findet, somit beispielsweise auch die Überwachung durch eine menschliche Person.[9] In Anbetracht dessen unterliegen auch nicht technikbasierte Kontrollmaßnahmen, wie etwa Befragungen und Beobachtungen durch Vorgesetzte, Tor-, Taschen- und Spindkontrollen[10] und der Einsatz eines Privatdetektivs[11] als Erhebung von persönlichen Daten des Mitarbeiters dem Datenschutzregime.[12] Nur wenn Kontrollmaßnahmen lediglich sachbezogene Infor- **7**

8 BAG, 29.6.2017 – 2 AZR 597/16, NZA 2017, 1179, Rn. 22.
9 *Maschmann*, NZA-Beil. 2018, 115, 115; *Seifert*, in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO, Art. 88 Rn. 71 f.
10 BAG, 20.6.2013 – 2 AZR 546/12, NZA 2014, 143, Rn. 24.
11 BAG, 29.6.2017 – 2 AZR 597/16, NZA 2017, 1179, Rn. 23.
12 ErfK/*Franzen*, § 26 BDSG Rn. 3; *Thüsing*, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 3 Rn. 33.

mationen liefern, müssen sie sich nicht an datenschutzrechtlichen Vorschriften messen lassen. So sind Sachstandsanfragen des Vorgesetzten und Berichtspflichten des Mitarbeiters über ihm übertragene Aufgaben ohne Weiteres zulässig.[13] Der Anwendungsbereich des Datenschutzrechts ist hier nicht eröffnet, weil die gewonnenen Erkenntnisse inhaltlich keinen Bezug zur Person des (kontrollierten) Mitarbeiters aufweisen, sondern sich ausschließlich auf den mitgeteilten Sachverhalt beziehen, indem sie diesen beschreiben.[14] Es handelt sich somit nicht um *personen*bezogene Daten. Solche liegen nur vor, wenn die Information ihrem Inhalt nach Rückschlüsse auf das Verhalten des Mitarbeiters oder dessen persönliche Merkmale oder Eigenschaften zulässt.[15] Bei der Mitarbeiterkontrolle im eigentlichen Sinne ist dies freilich stets der Fall.

3. Zulässigkeitsvoraussetzungen für Mitarbeiterkontrollen nach DSGVO und BDSG

8 Die DSGVO ist als Verbotsgesetz mit Erlaubnisvorbehalt konzipiert. Danach bedarf jede Verarbeitung personenbezogener Daten einer besonderen Rechtsgrundlage. Die zentralen Erlaubnistatbestände hierfür enthält Art. 6 Abs. 1 DSGVO, wonach u. a. die Einwilligung des Betroffenen (lit. a) die Datenverarbeitung rechtfertigt. Für Mitarbeiterkontrollen ist darüber hinaus die nationale Vorschrift des § 26 BDSG von besonderer Bedeutung. Mit der Vorschrift hat der deutsche Gesetzgeber den ihm in Art. 88 Abs. 1 DSGVO eingeräumten Regelungsspielraum zur Schaffung „spezifischerer Vorschriften" für die Datenverarbeitung im Beschäftigungskontext genutzt. Nach herrschender Auffassung konkretisieren die in § 26 BDSG enthaltenen Regelungen die allgemeineren Regelungen der DSGVO.[16]

9 Im Hinblick auf die Zulässigkeit von Mitarbeiterkontrollen ergibt sich somit folgendes Bild: Vorbehaltlich einer Einwilligung des Mitarbeiters, die in § 26 Abs. 2 BDSG nur partiell geregelt ist, müssen Kontrollmaßnahmen den Vorgaben der gesetzlichen Erlaubnistatbestände des § 26 BDSG genügen. Im Einzelfall, vor allem bei der vom Arbeitgeber erlaubten privaten Nutzung von Internet und E-Mail durch die Mitarbeiter, können darüber hinaus besondere datenschutzrechtliche Vorschriften aus dem TKG und TMG zu beachten sein. Insofern tritt das BDSG gegenüber einer abschließenden Regelung in den spezielleren Vorschriften des Bundes, dem TKG und TMG sowie dem BetrVG, zurück.[17]

---

13 *Maschmann*, NZA-Beil. 2018, 115, 115.

14 *Maschmann*, NZA-Beil. 2018, 115, 115; BeckOK DatenschutzR/*Schild*, Art. 4 DSGVO Rn. 22.

15 *Maschmann*, NZA-Beil. 2018, 115, 115.

16 ErfK/*Franzen*, § 26 BDSG Rn. 4 ff.; BeckOK DatenschutzR/*Riesenhuber*, Art. 88 DSGVO Rn. 15 f.; *Gräber/Nolden*, in: Paal/Pauly, DSGVO BDSG, § 26 BDSG Rn. 10 f.

17 *Maschmann*, NZA-Beil. 2018, 115, 116.

Allgemeine Kontrollgrundsätze im Rahmen der Mitarbeiterkontrolle sind einerseits der Verhältnismäßigkeitsgrundsatz, andererseits aber auch der Verantwortlichkeitsgrundsatz, der sich in § 26 Abs. 5 BDSG findet. Danach muss der für die Datenerhebung Verantwortliche die Einhaltung der in Art. 5 DSGVO dargelegten Grundsätze, namentlich **Rechtmäßigkeit der Datenverarbeitung**, **Zweckbindung**, **Datenminimierung**, **Richtigkeit**, **Speicherbegrenzung**, **Integrität** und **Vertraulichkeit** sicherstellen. Ferner muss der Verantwortliche gem. Art. 24 Abs. 1 DSGVO nicht nur technische und organisatorische Maßnahmen zur Gewährleistung einer DSGVO konformen Datenverarbeitung ergreifen, sondern er muss diese auch im Einzelnen nachweisen. Insofern ist gem. Art. 30 DSGVO ein **Verzeichnis aller Verarbeitungstätigkeiten** zu führen. Darüber hinaus ist in Art. 88 Abs. 2 DSGVO die Verpflichtung der Mitgliedstaaten zu angemessenen und besonderen Maßnahmen im Hinblick auf die Transparenz der Verarbeitung von Beschäftigtendaten normiert. Entsprechend den **allgemeinen Informationspflichten** der Art. 13–15 DSGVO muss der Beschäftigte im Zeitpunkt der Erhebung seiner personenbezogenen Daten klar erkennen und nachvollziehen können, ob, von wem und zu welchem Zweck seine Daten erhoben wurden. Demnach wären Maßnahmen wie etwa heimliche Videoüberwachungen im Hinblick auf einen Verstoß gegen das Transparenzgebot unzulässig.[18] Art. 23 Abs. 1 DSGVO sieht jedoch auch Beschränkungen des Transparenzprinzips vor, wie etwa zur Vermeidung oder Aufdeckung von Straftaten. Solche Beschränkungen dürfen die Mitgliedstaaten aber nur durch Gesetz anordnen.[19] **10**

a) Erlaubnistatbestand des § 26 Abs. 1 Satz 1 BDSG – Erforderlichkeit zur Durchführung des Arbeitsverhältnisses

Zentrale Vorschrift für die Überprüfung der Zulässigkeit von Mitarbeiterkontrollen ist § 26 Abs. 1 BDSG. Nach § 26 Abs. 1 Satz 1 BDSG ist die Verarbeitung personenbezogener Daten von Mitarbeitern zum Zwecke des Beschäftigungsverhältnisses u. a. dann zulässig, wenn dies für die **Durchführung des Beschäftigungsverhältnisses** erforderlich ist. Mag man auch Zweifel haben, ob die Leistungs- und Verhaltenskontrolle ihrem Zweck nach der „Durchführung" des Arbeitsverhältnisses dient, so ist trotz des unklaren Wortlauts unbestritten, dass solche Kontrollmaßnahmen auf § 26 Abs. 1 Satz 1 BDSG gestützt werden können.[20] Aufschluss gibt hier die Gesetzesbegründung zu dem insoweit wortlautidentischen § 32 Abs. 1 Satz 1 BDSG a. F. Danach soll die Vorschrift auch auf Datenverarbeitungen Anwendung finden, die der Arbeitgeber zum Zwecke der Wahrnehmung der mit der Durchführung des Beschäftigungsverhältnisses bestehenden Rechte vornimmt, z. B. durch Kontrollen der Leistung oder des Verhal- **11**

18 *Maschmann*, NZA-Beil. 2018, 115, 118.

19 *Maschmann*, NZA-Beil. 2018, 115, 118.

20 Vgl. nur BAG, 28.3.2019 – 8 AZR 421/17, NZA 2019, 1212, Rn. 35 zu dem insoweit wortlautidentischen § 32 BDSG a. F.; ErfK/*Franzen*, § 26 BDSG Rn. 22; *Thüsing*, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 3 Rn. 20.

tens der Mitarbeiter.[21] Da der Gesetzgeber bei der Schaffung von § 26 BDSG die bestehende Rechtslage fortschreiben und lediglich terminologische Anpassungen an die DSGVO vornehmen wollte,[22] kann nunmehr nichts anderes gelten. In diesem Sinne enthält auch Art. 88 DSGVO, von dem § 26 Abs. 1 Satz 1 BDSG seine Berechtigung ableitet, mit „Beschäftigungskontext" eine weitergehende Formulierung; in seinem zweiten Absatz sind sogar ausdrücklich Überwachungssysteme am Arbeitsplatz erwähnt.

12 Entscheidendes Zulässigkeitskriterium für Mitarbeiterkontrollen ist somit die **Erforderlichkeit**. Nach der Gesetzesbegründung sind im Rahmen der Erforderlichkeitsprüfung die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen. Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Allgemeine Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.[23] Die Rechtsprechung wendete hierzu im Rahmen von § 32 BDSG a. F. den Verhältnismäßigkeitsgrundsatz an.[24] Da die bestehende Rechtslage mit Schaffung von § 26 BDSG nicht verändert werden sollte, gilt dies auch weiterhin.[25] Der Verhältnismäßigkeitsgrundsatz ist zum einen zu beachten, wenn zu bestimmen ist, aus welchem **Anlass** kontrolliert werden darf und zum anderen, wenn es um die **konkrete Durchführung** einer Kontrolle geht. Somit beansprucht das Übermaßverbot hinsichtlich des „Ob" und des „Wie" einer Kontrollmaßnahme Geltung. Zur Wahrung des Verhältnismäßigkeitsgrundsatzes ist es beispielsweise relevant, wie viele Personen einer Kontrolle ausgesetzt sind und welche Nachteile aus der Überwachungsmaßnahme drohen. Im Rahmen der Erforderlichkeitsprüfung ist zudem zu bewerten, ob der Arbeitgeber nicht auf ein milderes, gleichgeeignetes Mittel zurückgreifen kann.[26]

13 Für den Arbeitgeber stellt sich die Frage, welche **präventiven Maßnahmen** ihm im Hinblick auf die Vermeidung möglicher Straftaten zustehen. Es geht also um den Bereich der **effektiven Compliance**. Nach der Gesetzesbegründung zur früheren Fassung des BDSG war die Zulässigkeit von Maßnahmen, die zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen erforderlich sind, die im Zusammenhang mit dem Beschäftigungsverhältnis stehen, nach § 32 Abs. 1 Satz 1 BDSG a. F. zu beurteilen.[27] Die Gesetzesbegründung zum aktuellen BDSG erwähnt zwar nicht explizit die Zulässigkeit von präventiven Maßnahmen nach § 26 Abs. 1 Satz 1 BDSG, jedoch wird man die Grundsätze zu § 32 BDSG a. F. auch hier übertragen können.[28] Präventive Kontrollen zur Vermeidung von

21 BT-Drs. 16/13657, 21.
22 BT-Drs. 18/11325, 96 f.
23 BT-Drs. 18/11325, 97.
24 Vgl. BAG, 20.6.2013 – 2 AZR 379/12, NZA 2014, 143, Rn. 26.
25 So auch ErfK/*Franzen*, § 26 BDSG Rn. 10; *Maschmann*, NZA-Beil. 2018, 115, 118.
26 BAG, 20.6.2013 – 2 AZR 546/12, NZA 2014, 143, Rn. 33.
27 BT-Drs. 16/13657, 21.
28 *Thüsing*, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 3 Rn. 26.

Straftaten lassen sich somit bei Vorliegen von dessen Voraussetzungen auf § 26 Abs. 1 Satz 1 BDSG stützen.[29] Es ist allerdings zu beachten, dass von § 26 Abs. 1 Satz 1 BDSG nur allgemeine Compliance-Maßnahmen gedeckt sind; sollten aus diesen Maßnahmen aber Informationen in Bezug auf einzelne Mitarbeiter resultieren, dann dürfen diese Informationen zur Verfolgung von Straftaten nur nach dem Maßstab des § 26 Abs. 1 Satz 2 BDSG weiterverfolgt und genutzt werden, also nur dann, wenn eine gewisse Erheblichkeit gegeben ist. Offen kommunizierte Überwachungsmaßnahmen des Arbeitgebers unterliegen aber unstreitig § 26 Abs. 1 Satz 1 BDSG.[30] Insofern ist auch die Zulässigkeit von Torkontrollen anhand von § 26 Abs. 1 Satz 1 BDSG zu bestimmen.[31]

b) Erlaubnistatbestand des § 26 Abs. 1 Satz 2 BDSG – Erforderlichkeit zur Aufdeckung einer Straftat

Gemäß dem Erlaubnistatbestand des § 26 Abs. 1 Satz 2 BDSG ist die Verarbeitung von personenbezogenen Daten dann zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine **Straftat** begangen hat, die Verarbeitung **zur Aufdeckung erforderlich** ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Auch innerhalb dieses Erlaubnistatbestands kommt es somit entscheidend auf die Erforderlichkeit der Datenerhebung sowie auf die Abwägung zwischen dem Aufklärungsinteresse des Arbeitgebers und der Persönlichkeitsbeeinträchtigung des Überwachten an.[32] Dabei ist die Intensität der Überwachungsmaßnahme mit der Dringlichkeit des Tatverdachts, der Zahl der überwachten Mitarbeiter sowie der Höhe des Schadens abzuwägen.[33] Folglich müssen die Maßnahmen dem Verhältnismäßigkeitsgrundsatz genügen.[34] Tatbestandlich erfordert § 26 Abs. 1 Satz 2 BDSG das Vorliegen von Straftaten, die im Beschäftigungsverhältnis begangen wurden, wobei ein unmittelbarer Bezug zur Leistungshandlung nicht vonnöten ist. Ordnungswidrigkeiten des Beschäftigten sind hingegen nicht von der gegenständlichen Norm erfasst. Auch Maßnahmen zur Aufdeckung von schwerwiegenden, aber nicht strafbaren Vertragsbrüchen, wie etwa Verstöße gegen das Wettbewerbsverbot, lassen sich nicht auf § 26 Abs. 1 Satz 2 BDSG stützen.[35] Die Zulässigkeit von Maßnahmen, die der Aufdeckung nicht strafbarer Verhaltensweisen des Mitarbeiters dienen, bestimmt sich somit nach § 26 Abs. 1 Satz 1 BDSG, wobei allerdings die strengeren Voraussetzungen des § 26 Abs. 1 Satz 2 **14**

29 ErfK/*Franzen*, § 26 BDSG Rn. 36.
30 *Thüsing*, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 3 Rn. 27.
31 ErfK/*Franzen*, § 26 BDSG Rn. 36; BAG, 9.6.2013 – 7 AZR 917/11, NZA 2013, 1433, Rn. 31.
32 ErfK/*Franzen*, § 26 BDSG Rn. 36.
33 ErfK/*Franzen*, § 26 BDSG Rn. 39.
34 ErfK/*Franzen*, § 26 BDSG Rn. 37.
35 *Thüsing*, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 3 Rn. 28.

BDSG bei repressiven Maßnahmen unterhalb der Strafbarkeitsschwelle im Rahmen der Zulässigkeitsprüfung nach § 26 Abs. 1 Satz 1 BDSG zu beachten sind.[36] Zudem erfordert eine Erhebung von personenbezogenen Daten nach § 26 Abs. 1 Satz 2 BDSG, dass **tatsächliche und nicht nur vage Anhaltspunkte für die Annahme einer begangenen Straftat** durch den Beschäftigten vorliegen.[37] Ein dringender Tatverdacht muss insofern aber nicht bestehen.[38] Im Vergleich zu § 26 Abs. 1 Satz 1 BDSG dient § 26 Abs. 1 Satz 2 BDSG der Aufklärung von Straftaten und damit repressiven Zwecken.[39] Im Übrigen kann auf die Grundsätze des § 100 TKG zurückgegriffen werden, denn § 26 Abs. 1 Satz 2 BDSG ist ebenso wie die Vorgängernorm des § 32 Abs. 1 Satz 2 BDSG a. F. der Vorschrift des § 100 TKG nachgebildet. Die Datenverarbeitung zu repressiven Zwecken unterliegt zusammengefasst strengeren Maßstäben als die Datenverarbeitung zu präventiven Zwecken.[40]

c) Erlaubnistatbestand des § 26 Abs. 2 BDSG – Einwilligung des Betroffenen

15 Ein Rechtfertigungsgrund für die Verarbeitung personenbezogener Daten stellt gem. § 26 Abs. 2 BDSG die Einwilligung des Betroffenen dar. Die Definition der Einwilligung findet sich in Art. 4 Nr. 11 und Art. 7 DSGVO, an die § 26 Abs. 2 BDSG anknüpft. Die Einwilligung muss grundsätzlich schriftlich (§ 126 BGB) oder elektronisch (d. h. im Ergebnis mit qualifizierter elektronischer Signatur, § 126a BGB) gegenüber dem Arbeitgeber erfolgen, § 26 Abs. 2 Satz 3 BDSG. Eine Einwilligung per Textform, also etwa per E-Mail, genügt somit nicht. Zudem ist das Merkmal der Freiwilligkeit der Einwilligung im Rahmen eines Arbeitsverhältnisses mit **hohen Anforderungen** verknüpft. Für die Beurteilung der **Freiwilligkeit** sind gem. § 26 Abs. 2 Satz 1 BDSG die Umstände zu berücksichtigen, unter denen die Einwilligung erklärt worden ist. Berücksichtigungswürdige Aspekte sind hierbei insbesondere die Eingriffstiefe und der Zeitpunkt der Erklärung der Einwilligung.[41] Eine freiwillige Einwilligung liegt gem. § 26 Abs. 2 Satz 2 BDSG insbesondere dann vor, wenn der Beschäftigte infolge der Datenverarbeitung einen rechtlichen oder wirtschaftlichen Vorteil erhält oder Arbeitgeber und Mitarbeiter gleichgerichtete Interessen verfolgen. Der Beschäftigte muss zudem seitens des Arbeitgebers über den Zweck der Datenverarbeitung **schriftlich aufgeklärt** werden. Eine bereits **bei Vertragsschluss erteilte Einwilligung** in die Mitarbeiterkontrolle, die sich in vielen Musterverträgen findet, **genügt nicht den Anforderungen** des § 26 Abs. 2 BDSG.[42] Die Einwil-

36 BAG, 29.6.2017 – 2 AZR 597/16, NZA 2017, 1179, Rn. 32.
37 ErfK/*Franzen*, § 26 BDSG Rn. 38.
38 BAG, 20.10.2016 – 2 AZR 395/15, NJW 2017, 1193, Rn. 25.
39 ErfK/*Franzen*, § 26 BDSG Rn. 36.
40 *Thüsing*, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 3 Rn. 23.
41 BT-Drs. 18/11325, 97.
42 *Maschmann*, NZA-Beil. 2018, 115, 116.

ligung ist somit generell nur selten als taugliche Grundlage für die Mitarbeiterkontrolle anzusehen.

d) Erlaubnistatbestand des § 26 Abs. 4 BDSG – Betriebsvereinbarungen

Beschäftigtendaten dürfen gem. § 26 Abs. 4 BDSG auf Grundlage von **Kollektivvereinbarungen**, insbesondere auf Grundlage einer Betriebsvereinbarung, verarbeitet werden. Die Vorschrift des § 26 Abs. 4 BDSG bestätigt die bisherige Rechtsprechung des BAG, das die Verarbeitung von Beschäftigtendaten auf Grundlage von Betriebsvereinbarungen oder Tarifverträgen für zulässig erachtete.[43] Im Rahmen der entsprechenden Kollektivvereinbarung ist gem. § 26 Abs. 4 Satz 2 BDSG die Vorschrift des Art. 88 Abs. 2 DSGVO zu beachten, wonach besondere und angemessene Maßnahmen zur Wahrung der berechtigten Interessen und Grundrechte der betroffenen Personen zu berücksichtigen sind. Insofern muss in einer solchen Betriebsvereinbarung ein **angemessener Ausgleich** zwischen den Arbeitgeberinteressen und den schutzwürdigen Belangen des Mitarbeiters gewährleistet werden.[44] Dem entspricht im deutschen Recht die Vorschrift des § 75 Abs. 2 Satz 1 BetrVG. Eine solche Betriebsvereinbarung muss also inhaltlich ebenfalls dem Verhältnismäßigkeitsgrundsatz genügen, sodass auch in diesem Rahmen wieder eine Güterabwägung zwischen dem Persönlichkeitsrecht des Mitarbeiters und den schutzwürdigen Interessen des Arbeitgebers vorzunehmen ist. Ob durch Betriebsvereinbarungen auch Verschärfungen der Regeln zur Mitarbeiterkontrolle im Vergleich zu den Regeln der DSGVO möglich sind, ist umstritten. Der überwiegenden Auffassung nach können Betriebsvereinbarungen auch strengere Grundsätze als die DSGVO aufstellen, was mit dem Wortlaut des Art. 88 Abs. 1 DSGVO, der spezifischere Vorschriften der Mitgliedstaaten im Beschäftigtendatenschutz erlaubt, begründet wird.[45] Konträr dazu sind einer anderen Ansicht nach strengere nationale Regelungen im Vergleich zu denjenigen der DSGVO trotz der Öffnungsklausel des Art. 88 Abs. 1 DSGVO nicht erlaubt, um so ein unionsweit gleichmäßiges und einheitliches Datenschutzrecht zu gewährleisten.[46] Für das Prinzip der Vollharmonisierung spricht unter anderem auch, dass strengere Regeln auf nationaler Ebene, wie etwa ein vollständiger Ausschluss jeder Leistungs- und Verhaltenskontrolle, unter dem Stichwort der Compliance problematisch wären, da der Arbeitgeber dazu verpflichtet ist, rechtswidrige Handlungen seiner Mitarbeiter zu verhindern bzw. aufzudecken.[47] **16**

---

43 BAG, 25.6.2002 – 9 AZR 405/00, NZA 2003, 275, 279; BAG, 27.5.1986 – 1 ABR 48/84, AP BetrVG 1972 § 87 Überwachung Nr. 15.

44 ErfK/*Franzen*, § 26 BDSG Rn. 48.

45 So zum Beispiel: *Düwell/Brink*, NZA 2016, 665, 668; *Kort*, ZD 2017, 319, 321 f.

46 *Maschmann*, NZA-Beil. 2018, 115, 117; *Franzen*, EuZA 2017, 313, 346; *Wybitul*, NZA 2017, 413, 413.

47 *Maschmann*, NZA-Beil. 2018, 115, 117.