# Kapitel 6
# Verarbeitungen im Rahmen der Durchführung des Beschäftigungsverhältnisses (§ 26 Abs. 1 S. 1 BDSG) (II) – Digitalisierte Steuerung und Kontrolle von Beschäftigten

## 1 Vorbemerkung

### 1.1 Digitalisierung

Die Erlaubnisnorm des § 26 Abs. 1 S. 1 Var. 1 BDSG erlaubt Verarbeitungen, die für *„die Durchführung des Beschäftigungsverhältnisses erforderlich sind"*. Geprägt wird der Zulässigkeitstatbestand durch die Reichweite des Begriffs der „Durchführung" einerseits und die Begriffe der **„Erforderlichkeit"** und Verhältnismäßigkeit andererseits. **1085**

*Vgl. hierzu im Einzelnen Kap. 5, RN 746.*

Datenschutz im Arbeitsverhältnis verdichtet sich bei dem Einsatz der Datenverarbeitungstechnik als Mittel der Überwachung und Steuerung des Verhaltens der Beschäftigten. Dabei steht **Digitalisierung** als Schlagwort für die informationstechnologisch getriebenen Veränderungen von Wirtschaft und Arbeit insgesamt und auch die neuen Möglichkeiten technischer Steuerung und Kontrolle des Verhaltens der Beschäftigten konkret. **1086**

*Krause, Digitalisierung und Beschäftigtendatenschutz, BMAS-Forschungsbericht 482, 2017; Däubler, Digitalisierung und Arbeitsrecht, 2018*

Über 80 Prozent der Beschäftigten in Deutschland nutzen in ihrer beruflichen Tätigkeit aktuell digitale Informations- oder Kommunikationstechnologie. In den 1990ern begann der Siegeszug des Internets, in den 2000er Jahren die Ära der mobilen Endgeräte Die Technologien, die den digitalen Strukturwandel vorantreiben, werden sich schnell weiterentwickeln, wobei **künstliche Intelligenz** der Maschinen dem Menschen das Denken abnimmt und für ihn nicht erkennbare Zusammenhänge und Entwicklungen aufdeckt. **1087**

*DuD, Conrad, Künstliche Intelligenz – Die Risiken für den Datenschutz, DuD 2017, 740*

Jeder Einsatz von digitaler Technik erlaubt das Verhalten ihres Nutzers festzuhalten und zu kontrollieren, gleichgültig, ob dies das unmittelbare Ziel sein oder auch nur eine Nebenfolge ist. **1088**

Automatisierte Mitarbeiterkontrollen in Gestalt von **Zeiterfassungs- und Zugangskontrollsystemen** **1089**

*zu den Einzelheiten vgl. Byers, Mitarbeiterkontrollen, RN 113 ff.*

sind langjährige betriebliche Praxis. Ihre Einführung liegt, sofern die betriebliche Organisation sie erfordert, im **Direktionsrecht** des Arbeitgebers,

*BAG, Urt. v. 19.02.2015 – 8 AZR 1007, 13 = ZD 2015, 380; zu alledem ausführlich Däubler, Digitalisierung und Arbeitsrecht, § 7, RN 77 ff.*

wobei die Verwendung biometrischer Daten besonderer Rechtfertigung bedarf.

*Vgl. Kap. 11, RN 1845; Gola, Aus den Berichten der Aufsichtsbehörden (38), RDV 2018, 315*

**1090** Durch die fortschreitende **Digitalisierung** wird ein Arbeitgeber jedoch im umfassenderen Maße in die Lage versetzt, seine Beschäftigten nahezu **lückenlos zu überwachen**.

*BMAS: Weißbuch „Arbeiten 4.0", 2017, 142*

**1091** Z.B. ermöglichen **Login-Daten** die Kontrolle: Wer hat wann, an welchem Arbeitsplatz wie lange eine Akte mit welchem Inhalt überarbeitet? Zur **Lokalisierung** von Beschäftigten

*zur Überwachung bei mobiler Arbeit vgl. Göpfert/Papst, DB 2016, 1015*

innerhalb von Betriebsstätten kommen vorwiegend **RFID-Systeme** zum Einsatz.

*Vgl. DSK-Orientierungshilfe „Datenschutzgerechter Einsatz von RFID"*

**1092** Außerhalb von Betriebsstätten stehen die Ortung von Mobilfunkendgeräten (**Handy-Ortung**) sowie die Übermittlung von **GPS-Positionsdaten** im Vordergrund.

*Sieling/Philipp, Die Zulässigkeit von Ortungssystemen, ITRB 2013, 255*

**1093** Verwendungszweck ist vielfach das **Flottenmanagement**.

*Schröder, Arbeitnehmerdatenschutz beim Fleetmanagement, ZD 2013, 13*

**1094** Speziell gesetzlich geregelt ist die **Handy-Ortung**. Der Arbeitgeber hat den Mitarbeiter über den von ihm mit dem Telekommunikationsdienstleister getroffenen Modus (§ 98 Abs. 1 TKG) zu unterrichten (§ 98 Abs. 15.2 TKG). Über die Zulässigkeit der Ortung besagt die Bestimmung jedoch nichts. Diese richtet sich nach § 26 Abs. 1 BDSG.

**1095** Vorgeschrieben ist der digitale **Tachograf** für Lkws und Busse. Der Arbeitgeber muss die aufgezeichneten Daten zwei Jahre lang aufbewahren.

*Vgl. nachfolgend RN 1246*

**1096** Nachgewiesen werden können muss auch die regelmäßige **Führerscheinkontrolle**.

*Vgl. nachfolgend RN 1235*

**1097** Neue Anwendungen wie etwa Stimmungs- und **Sprachanalyseverfahren**

*Vgl. nachfolgend RN 1137*

oder Auswertungen betrieblicher sozialer Netzwerke hinsichtlich des **„sozialen Graphen"** erlauben die Persönlichkeit von Arbeitnehmern zu durchleuchten, um eine Bewertung über sie abzugeben oder ihr zukünftiges Verhalten zu berechnen.

*Vgl. nachfolgend RN 1145*

## 1.2 Big Data für das Personalmanagement

**1098** Unabhängig von der im Detail unterschiedlichen Definition des Begriffs in der Fachwelt werden seit Längerem **Business-Intelligence-Systeme** diskutiert und praktiziert. Durch Verfahren und Prozesse zur systematischen Analyse von – in der Regel im Unternehmen – vorhandenen Daten sollen neue Erkenntnisse zur Verwirklichung der Unternehmensziele gewonnen werden. Ziel ist es, Geschäftsabläufe sowie Kunden- und Lieferantenbeziehungen profitabler zu machen, d.h. Kosten zu senken, Risiken zu minimieren und die Wertschöpfung zu vergrößern.

Business Intelligence bezeichnet ein integriertes Gesamtkonzept, das unterschiedliche Technologien und Konzepte zusammenfasst, die der Sammlung und Aufbereitung

unternehmensinterner und -externer Daten dienen und diese in Form von geschäftsrelevanten Informationen transparent und verständlich zur Analyse und Entscheidungsunterstützung bereitstellen.

*Entnommen bei Hilbert/Müller, Business Intelligence bei Entscheidungen im Human Resource Management, S. 69.*

Unter dieser Vorgabe kann Business Intelligence auch dem Personalmanagement aus der ständig zunehmenden Masse an Beschäftigtendaten Informationen über den „Human Capital Value" des Unternehmens bereitstellen und speziell im Bereich des **Human Resource Controlling** die Planung, Bewertung und Steuerung sowohl der Mitarbeiter als auch der Personalarbeit an sich optimieren. **1099**

Eine weitgehend deckungsgleiche Thematik beschreibt der inzwischen schon wieder etwas inflationär gewordene Begriff **„Big Data"**. **1100**

*Weichert, Big Data und Datenschutz – Chancen und Risiken einer neuen Form der Datenanalyse, ZD 2013, S. 251*

Ausgangspunkt sind die durch das Internet und die immer stärker werdende Nutzung der Informationstechnik ständig zunehmenden Dimensionen von Datenbeständen und das Bestreben, Technologien zu entwickeln, um die weitgehend unstrukturierten Datenbestände durchsuchen, analysieren und visualisieren zu können. Als neue, attraktivste Datenquelle sind inzwischen **soziale Netzwerke** zu verzeichnen, deren Geschäftsbasis auf der Vermarktung der Daten ihrer Nutzer aufbaut. **1101**

Der Bitkom-Arbeitskreis Big Data formuliert dahingehend: *„Big Data bezeichnet die wirtschaftliche sinnvolle Gewinnung und Nutzung entscheidungsrelevanter Erkenntnisse aus qualitativ vielfältigen und unterschiedlich strukturierten Informationen, die einem schnellen Wandel unterliegen und in bisher unbekanntem Umfang anfallen. Big Data stellt Konzepte, Methoden, Technologien, IT-Architekturen sowie Tools zur Verfügung, um die geradezu exponentiell steigenden Volumina vielfältiger Informationen in besser fundierte und zeitnahe Managemententscheidungen umzusetzen und so die Innovations- und Wettbewerbsfähigkeit von Unternehmen zu verbessern."*

*www.bitkom.org/de/wir_uns/70822*

Nicht mehr die Menge der Daten, sondern die neuen Möglichkeiten ihrer Nutzung sind das maßgebende Kriterium. Dabei geht es um die Entwicklung von **Algorithmen**, d.h. Verfahrensweisen zum Erkennen und Lösen von ggf. sich erst abzeichnenden Problemen. Damit ist nach wie vor auch im aktuellen „Big Data"-Umfeld der das Auswerten großer Datenmengen bezeichnende Begriff des **Data Mining** problembeschreibend. **1102**

Als Data Mining bezeichnet man Verfahren zur Analyse großer Datenbestände, die aus der unübersehbaren Fülle von Details bisher unbekannte Strukturen und Zusammenhänge herausfiltern und diese Informationen so aufbereiten und bewerten, dass sie eine verbindliche Entscheidungshilfe darstellen,

*Grund, Wertvolles Wissen entdecken und Risiken vermeiden – Data Mining in der Praxis, in: Deggendorfer Forum zur digitalen Datenanalyse e.V. (Hrsg.), Big Data – Systeme und Prüfung, Fußnote 23, S. 23*

deren Spielart sog. unstrukturierte Daten auswertbar macht.

Viele der auszuwertenden Daten sind personenbezogen und können in ein individuelles Scoring, Tracking oder Profiling einfließen. Durch das **Tracking** werden unter Auswertung von Mobilfunkdaten oder per GPS Bewegungsdaten einer Person, d.h. ihre jewei- **1103**

ligen Aufenthaltsorte verfolgt. Das mit dem Begriff des **Targeting** beschriebene Nachverfolgen von Bewegungen im Internet macht nicht nur das Konsumverhalten berechenbar. Auch Erkenntnisse über den **Bildungsstand**, die politische Einstellung etc. sind ablesbar. **Fraud-Analysen** zur Aufdeckung von Insidergeschäften werden in Echtzeit ermöglicht, wie es bei Mitarbeitern an der Kasse hinsichtlich auf einschlägigen Erfahrenserkenntnissen basierenden **Kassenprüfungssystemen** der Fall ist.

*Vgl. Derksen, Fraud-Analysen von Massendaten in Echtzeit in: Big Data, S. 45; hierzu nachfolgend RN 1154, 1396.*

**1104** Obwohl Big Data eine der zentralen Herausforderungen des Datenschutzes ist, bleibt es in der DS-GVO ohne jede Erwähnung.

*Vgl. hierzu Schulz in: Gola (Hrsg.), DS-GVO, Art. 6, RN 254.*

**1105** Relevanz entfaltet die DS-GVO jedoch dadurch, dass sie die regelmäßig einer der ursprünglichen Zweckbestimmung der Daten nachfolgende – ggf. noch offenen Zwecken dienende – Analyse zunächst mit dem Gebot der Zweckbindung als unvereinbar ansieht und für diesbezügliche Weiterverarbeitung Erlaubnistatbestände fordert,

*vgl. hierzu nachstehend Kap. 14, RN 2295*

wobei den Instrumenten der **Anonymisierung**, und **Pseudonymisierung** zentrale Bedeutung zukommt, da echte Big Data-Analysen, die ergebnisoffen mit dem Ziel der Mustererkennung oder der Generierung neuer (personenbezogener) Informationen und insoweit ohne konkrete oder mit sich **verändernder Zweckbestimmung** („Embedded Analytics“) erfolgen, nur ausnahmsweise als zulässig erachtet werden können.

*Vgl. auch Deutscher Ethikrat, Big Data und Gesundheit, Stellungnahme, 2017, S. 97.*

Dabei ist dann für die Zulässigkeit der Verarbeitung die Wirksamkeit der eingesetzten Maßnahmen zum Schutz vor Reidentifizierung maßgeblich.

*Zu der dann entfallenden Anwendung der DS-GVO vgl. Schulz in: Gola, DS-GVO, Art. 6, RN 257.*

## 1.3 Sonderproblem: „Bring your own device (BYOD)“

### 1.3.1 Allgemeines

**1106** Mit einem offensichtlich nicht zu vermeidenden englischen Begriff des **„Bring your own Device – BYOD“** wird die Nutzung von privaten „Vorrichtungen“ wie z.B. Notebooks, Tablet-PCs oder Smartphones zu dienstlichen Zwecken bezeichnet, wobei diese Geräte Zugriff auf die IT-Ressourcen des Unternehmens erhalten. Gemeint ist aber auch die Verwendung privater Software. Der Einsatz eigener digitaler Technik beruht zumeist auf dem Wunsch des Mitarbeiters, so z.B. weil der Arbeitgeber ihm keine oder nicht die gewünschte Technik zur Verfügung stellt. Der typische Fall des **BYOD** liegt darin, dass der Arbeitgeber dem Mitarbeiter gestattet, sein Smartphone, das Laptop oder Tablet – ggf. neben dem privaten – auch für den dienstlichen Einsatz im Betrieb zu nutzen. Eine einfache BYOD-Nutzung liegt auch vor, wenn dienstlicher E-Mail-Verkehr nach Dienstschluss vom privaten Computer aus abgewickelt wird. Problematischer wird der Einsatz privater Geräte, wenn sie Zugang zu dem firmeninternen Netzwerk haben. Als „unechtes“ BYOD wird der teilweise gleichgelagerte Fall bezeichnet, dass der Arbeitgeber dem Mitarbeiter gestattet, arbeitgebereigene Endgeräte auch für private Zwecke zu verwenden.

*Franck, Bring your own Device – rechtliche und tatsächliche Aspekte, RDV 2013, 185; Söbbing, Rechtsrisiken durch Bring your own Device (BYOD) – Wie man mit privatem IT-Equipment rechtssicher im Unternehmen arbeiten kann, RDV 2013, 77*

*Vgl. im Einzelnen bei Helfrich in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil IV, RN 4 ff.*

**1107** Der Arbeitgeber kann zwar die Anschaffung oder den Einsatz privater Kommunikationstechnik nicht per Direktionsrecht anordnen – § 106 GewO hat keine solche Anordnungsreichweite.

*Zöll/Kielkowski, Arbeitsrechtliche Umsetzungon „Bring your own Device" (BYOD);BB 2012, 2625; Conrad/Schneider, Einsatz von „privater IT" im Unternehmen, ZD 2013, 153*

Andererseits steht außer Frage, dass der Arbeitnehmer zum Einsatz seiner **privaten Hard- und Software** ohne Erlaubnis des Arbeitnehmers nicht berechtigt ist.

*Vgl. BAG, Urt. v. 24.03.2011 – 2 AZR 282/10 = RDV 2011, 300 zur unbefugten Speicherung dienstlicher Daten auf privatem PC*

Es bedarf einer individuellen, **AGB-festen** Vereinbarung.

*Zum Inhalt vgl. Arning/Moos/Becker, Vertragliche Absicherung von Bring your own Device, CR 2012, 592.*

**1108** Der Abschluss einer solchen Vereinbarung kann jedoch zur **Conditio für den Abschluss des Arbeitsvertrags** gemacht werden. Hierbei handelt es sich um eine Nebenabrede, durch die der Arbeitgeber jedoch nicht unangemessen benachteiligt werden darf (§ 307 Abs. 1 BGB),

*Däubler, Digitalisierung und Arbeitsrecht, RN 210 f und g*

was einerseits z.B. die anteilige Übernahme evtl. Nutzungskosten bedingt und andererseits die Berücksichtigung des Verhältnismäßigkeitsprinzips bei der erforderlichen Regelung des Kontrollbedarfs seitens des Arbeitgebers.

*Zur Überwachung bei mobiler Arbeit vgl. Göpfert/Papst, DB 2016, 1015; zum Einsatz privater Smartphones für dienstliche Zwecke vgl. Göpfert/Wilke, NZA 2012, 765.*

**1109** Eine Pflicht des Arbeitnehmers zur Einbringung privater Geräte kann auch nicht durch Betriebsvereinbarung begründet werden. Diese kann sich jedoch darauf beziehen, welche Kontrollmechanismen bei der eingewilligten betrieblichen Nutzung dem Arbeitgeber (§ 87 Abs. 1 Nr. 6 BetrVG) bzw. welche Einsatzmöglichkeiten dem Mitarbeiter gestattet sind (§ 87 Abs. 1 Nr. 1 BetrVG) und wie die gegenseitigen Verantwortlichkeiten verteilt sind.

*Däubler, Digitalisierung und Arbeitsrecht, § 3, RN 9 ff.*

### 1.3.2 Anwendung datenschutzrechtlicher Vorschriften

**1110** Im Rahmen des BYOD erfolgt regelmäßig eine Nutzung der Technik für nicht unter die Datenschutznormen der DS-GVO bzw. des BDSG fallende persönliche und familiäre Zwecke einerseits (Art. 2 Abs. 2 lit. c DS-GVO) und dienstliche Zwecke andererseits. Findet keine **organisatorische Trennung** zwischen beiden Bereichen statt, „infiziert" der dienstliche Zweck datenschutzrechtlich die private Nutzung.

*Helfrich in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil IV, RN 27, auch zu den privaten Nutzungsfällen.*