Tim Wybitul, RA/FAArbR

Wie viel Arbeitnehmerdatenschutz ist „*erforderlich*“?

– Erfahrungen und Empfehlungen zum Umgang mit dem neuen § 32 BDSG –

Seit dem 1.9.2009 ist eine neue Regelung zum Arbeitnehmerdatenschutz in Kraft. Der Umgang mit personenbezogenen Daten von Beschäftigten muss stets dem Kriterium der „Erforderlichkeit“ genügen. Der vorliegende Beitrag beschreibt anhand von Beispielen die Auswirkungen für die betriebliche Praxis. Er zeigt Erlaubtes und Verbote auf und gibt konkrete Empfehlungen zum Umgang mit dem Tatbestandsmerkmal „erforderlich“ bei Personalarbeit und Themen der Compliance. Eine Checkliste zum praktischen Umgang mit § 32 BDSG vervollständigt den Überblick.

I. Der neue § 32 BDSG

Das BDSG verbietet den Umgang mit personenbezogenen Daten[1], wenn nicht das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder wenn der Betroffene eingewilligt hat[2]. Der neue § 32 BDSG ist die maßgebliche Bestimmung für den Umgang mit Daten im Arbeitsverhältnis[3]. Diese Regelung gilt nicht allein für Arbeitnehmer, sondern für alle Beschäftigten. § 3 Abs. 11 BDSG bestimmt den Begriff des Beschäftigten: Neben Arbeitnehmern umfasst er unter anderem Auszubildende, Heimarbeiter, Bewerber und ehemalige Beschäftigte, Beamte, Richter, Soldaten und Zivildienstleistende. An § 32 BDSG wird kritisiert, die Regelung sei unklar[4], eine „Verschlimmbesserung“[5], ein „funktionsloses Schaustück des Reformwillens“[6], sie erschwere die Korruptionsbekämpfung[7] und veranlasse Unternehmen, im Bereich Compliance erst einmal untätig zu bleiben[8] und abzuwarten, bis Klarheit über Erlaubtes und Verbotenes besteht. *Barton* fasst die Situation treffend zusammen: „*Kritikpunkte sind angesichts der kryptischen Formulierung des § 32 Abs. 1 BDSG im Überfluss vorhanden.*“[9]

Dieser Beitrag zeigt Möglichkeiten auf, bestehende Unsicherheiten zu verringern und schildert praxisorientierte Vorgaben zum Umgang mit dem neuen Arbeitnehmerdatenschutz.

II. Umgang mit Daten von Beschäftigen für „Zwecke des Beschäftigungsverhältnisses“

Nach § 32 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses nur unter engen Voraussetzungen erhoben, verarbeitet oder genutzt werden. § 32 BDSG erlaubt diesen Umgang mit personenbezogenen Daten nur dann, wenn dies für die Entscheidung über die Begründung oder Beendigung oder für die Durchführung eines Beschäftigungsverhältnisses „*erforderlich*“ ist.

PRAXISTIPP: Das BDSG – und damit das Erfordernis der Erforderlichkeit – gilt seit der BDSG-Novelle 2009 für weitgehend jeden Umgang mit Arbeitnehmerdaten[10], wie etwa manuell geführte Personalakten, Befragungen von Arbeitnehmern oder Notizen des Arbeitgebers[11]. Denn der neu eingeführte § 32 Abs. 2 BDSG legt fest, dass bei Daten von Beschäftigten die sonst im BDSG geltende Beschränkung[12] auf dateimäßige oder automatische Datenverarbeitung[13] nicht gilt.

Das Gesetz liefert keine näheren Anhaltspunkte, welche Vorgehensweisen im Einzelnen erforderlich sind und welche nicht. Laut der Gesetzesbegründung entspricht die gesetzliche Regelung den von der Rechtsprechung entwickelten Grundsätzen zum Datenschutz im Beschäftigungsverhältnis[14].

Beispiele: Als erforderliche Handlungen nennt der Gesetzgeber Fragen im Bewerbungsgespräch, etwa nach fachlichen Fähigkeiten, Kenntnissen und Erfahrungen. Arbeitgeber dürfen Daten verwenden, um ihre arbeitsvertraglichen Pflichten zu erfüllen, z. B. bei Personalverwaltung, Lohn- und Gehaltsabrechnung[15]. Auch Kontrollen der Leistung oder des Verhaltens der Arbeitnehmer fallen nach der Gesetzesbegründung unter § 32 Abs. 1 S. 1 BDSG, etwa zur Verhinderung von Straftaten[16] oder sonstigen Rechtsverstößen, die im Zusammenhang mit dem Beschäftigungsverhältnis stehen. Bei Maßnahmen zur Prävention von Straftaten oder bei allgemeinen Kontrollen gilt die allgemeine Vorschrift des § 32 Abs. 1 S. 1 BDSG. Lediglich bei Maßnahmen zur Aufdeckung konkreter, bereits begangener Straftaten kommt die strengere Regelung des § 32 Abs. 1 S. 2 BDSG zur Anwendung[17].

Dass Personalverwaltung und Leistungskontrollen weiterhin erlaubt sind, ist zwar beruhigend, hilft aber bei Fragen der täglichen Personalarbeit oder gar bei Themen der Compliance kaum weiter. Daher werden nachstehend Lösungsansätze aufgezeigt, die das maßgebliche Kriterium der Erforderlichkeit näher bestimmen.

1 Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene), § 3 Abs. 1 BDSG. Einen guten Überblick über die Einzelheiten zu personenbezogenen Daten geben Kühling/Seidel/Sivridis, Datenschutzrecht, 1. Aufl. 2008, S. 102.
2 § 4 Abs. 1 BDSG.
3 Vgl. zu den Hintergründen der Einführung von § 32 BDSG *Thüsing*, NZA 2009, 865, 865 ff.
4 *Gola/Jaspers*, RDV 2009, 213, 213, vgl. auch *Wybitul*, BB 2009, 1582, 1584.
5 *Barton*, DRV 2009, 200, 202.
6 *Thüsing*, NZA, 2009, 865, 870 nennt § 32 BDSG mit guter Begründung auch einen „*Eyecatcher gesetzgeberischen Handelns*“.
7 Handelsblatt vom 6.7.2009, S. 19, Datenschutz schwächt Korruptionsbekämpfung.
8 Handelsblatt vom 26.9.2009, S. 11, Kriminelle im Anzug haben es leicht.
9 *Barton*, RDV 2009, 200, 202.
10 Das gilt nicht für den Umgang mit Daten ausschließlich für persönliche oder familiäre Tätigkeiten, § 27 Abs. 1 S. 2 BDSG.
11 So auch Däubler, in Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 32 Rn. 5.
12 § 27 Abs. 1 S. 1 Nr. 1 BDSG.
13 Vgl. § 3 Abs. 2 BDSG.
14 BT-Drs. 16/13657, S. 21.
15 BT-Drs. 16/13657, S. 21.
16 Vgl. *Schmidt*, RDV 2009, 193, 196.
17 Vgl. *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 32 Rn. 125 ff.

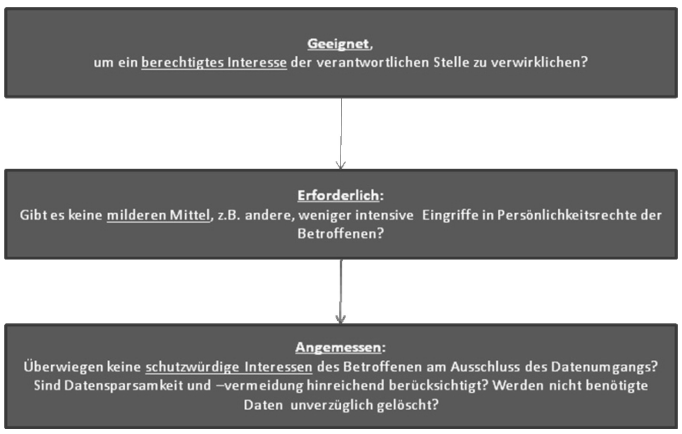
III. Einzelheiten zur Erforderlichkeit – welcher Umgang mit Beschäftigtendaten ist zulässig?

In der Praxis ist es für den Datenanwender im Betrieb nicht einfach, festzustellen, welcher Umgang mit Beschäftigtendaten erforderlich ist. Einen wichtigen Anhaltspunkt gibt die Gesetzesbegründung. Danach soll § 32 Abs. 1 S. 1 BDSG den bisher von der Rechtsprechung aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Grundsätzen zum Datenschutz im Beschäftigungsverhältnis entsprechen[18]. Mit anderen Worten: Erforderlich soll jeweils der Datenumgang sein, den Bundesarbeitsgericht und Bundesverfassungsgericht bereits in der Vergangenheit als zulässig erachtet haben.

Tatsächlich lassen sich der bisherigen Rechtsprechung zur Erhebung, Verarbeitung und Nutzung von Arbeitnehmerdaten einige Anhaltspunkte entnehmen, anhand derer sich der Begriff der Erforderlichkeit näher bestimmen lässt. Die Rechtsprechung wägt berechtigte Interessen des Arbeitgebers an dem Umgang mit den Personaldaten gegen die betroffenen Rechtsgüter der betroffenen Beschäftigten ab. Maßgeblich für die hierbei vorzunehmende Interessenabwägung ist der Grundsatz der Verhältnismäßigkeit[19]. Dem tragen auch die in § 3a BDSG geregelten Grundsätze der Datenvermeidung und Datensparsamkeit Rechnung[20]. Nach dieser Regelung sollen so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit das nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck un*verhältnismäßigen* Aufwand erfordert[21].

IV. Grundsatz der Verhältnismäßigkeit im Beschäftigungsverhältnis

Der vom BAG in Bezug genommene Grundsatz der Verhältnismäßigkeit[22] verlangt, dass die Maßnahme einem *legitim*en Zweck dient, *geeignet, erforderlich* und unter Berücksichtigung des Persönlichkeitsrechts des Arbeitnehmers *angemessen* ist, um den erstrebten Zweck zu erreichen[23]. Auch in der Literatur zum Datenschutzrecht ist der Verhältnismäßigkeitsgrundsatz als tragendes Prinzip des BDSG anerkannt[24]. § 32 Abs. 1 S. 2 BDSG nimmt ausdrücklich auf das Erfordernis der Verhältnismäßigkeit Bezug[25]. Mittels der diesen Grundsatz näher bestimmenden Kriterien Geeignetheit, Erforderlichkeit und Angemessenheit ist eine Vielzahl von konkreten Vorgaben für die Anwendung von § 32 BDSG in der betrieblichen Praxis zu gewinnen.



1. Geeignetheit

Geeignet ist eine Maßnahme, wenn mit ihrer Hilfe der vom Arbeitgeber angestrebte Zweck gefördert werden kann[26]. Dieser Zweck muss sich auf die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder auf die Durchführung oder die Beendigung des Beschäftigungsverhältnisses beziehen[27]. Sinnvollerweise ist bereits bei der Prüfung der Geeignetheit zu fordern, dass es sich um einen von der Rechtsordnung gebilligten Zweck handelt.

Beispiel: Das Sammeln von Daten, um einen Grund für die Kündigung eines Arbeitnehmers zu finden, der die Gründung eines Betriebsrats forciert, ist nicht für einen der in § 32 Abs. 1 S. 1 BDSG genannten Zwecke geeignet und damit nicht zulässig. Ebenso sind Maßnahmen nicht geeignet, mit denen der angestrebte Zweck objektiv nicht erreicht werden kann.

2. Erforderlichkeit

Der Begriff der Erforderlichkeit im Rahmen der Rechtsprechung des Bundesarbeitsgerichts ist nicht deckungsgleich mit der in § 32 BDSG geforderten „Erforderlichkeit". Bei der vorliegenden Prüfung geht es um eine Erforderlichkeit im engeren Sinne. In diesem Zusammenhang ist der Umgang mit Beschäftigtendaten erforderlich, wenn kein anderes, gleich wirksames und die Persönlichkeitsrechte der Betroffenen weniger einschränkendes Mittel zur Verfügung steht[28]. Der Arbeitgeber muss allerdings keine Mittel wählen, die weniger effizient, organisatorisch aufwendiger oder unwirtschaftlicher sind, insoweit muss auch der Datenschutz der unternehmerischen Freiheit Rechnung tragen[29].

Beispiel: Heimliche Kontrollmaßnahmen (z. B. Videoüberwachung) sind nach der Rechtsprechung einschneidender als solche, die den Beschäftigten bekannt sind[30]. Kann das angestrebte Ziel durch einen den Betroffenen bekannten Datenumgang erreicht werden, ist ein heimliches Vorgehen nicht erforderlich und damit nach § 32 BDSG nicht zulässig. Besonders problematisch ist das Erheben von Daten ohne Kenntnis der betroffenen Beschäftigten. Denn personenbezogene Daten sind beim Betroffenen selbst zu erheben, wenn nicht einer der in § 4 Abs. 2 S. 2 BDSG geregelten Ausnahmefälle vorliegt.

3. Angemessenheit

Die Feststellung, ob ein konkretes Vorgehen angemessen ist oder nicht, beruht auf einer Abwägung der betroffenen Interessen[31]. In den meisten Fällen werden wirtschaftliche Interessen des Arbeitgebers

18 BT-Drs. 16/13657, S. 21.
19 BAG, BB 1987, 1461 Rn. 31. BAG, NZA 2008, 1187 Rn. 17.
20 Vgl. *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 3 Rn. 1.
21 § 3a S. 2 BDSG.
22 Vgl. BVerfG, NJW 2006, 1939 Rn. 82.
23 *Di Fabio*, in: Maunz-Dürig, GG, Art. 2 Abs. 1 Rn. 41; *Kock/Franke*, NZA 2009, 646, 648; *Löwisch*, DB 2009, 2782, 2785; *Schmidt*, RDV 2009, 193, 196.
24 *Gola/Klug*, Grundzüge des Datenschutzrechts, Aufl. 2003, S. 46; vgl. *Gola/Jaspers*, Das novellierte BDSG im Überblick, 5. Aufl. 2010 zu § 28 Abs. 1 S. 1 Nr. 1: *„Maßgebend für die bei Datenspeicherungen im Rahmen eines Vertragsverhältnisses insoweit zu beachtende Zweckbestimmung ist der Grundsatz der Verhältnismäßigkeit."*
25 § 32 Abs. 1 S. 2 BDSG: *„… und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind."*
26 Vgl. *Di Fabio*, in: Maunz-Dürig, GG, Art. 2 Abs. 1 Rn. 41; BAG, NZA 2008, 1187 Rn. 19.
27 Dies ergibt sich unmittelbar aus dem Wortlaut von § 32 Abs. 1 S. 1 BDSG.
28 *Di Fabio*, in: Maunz-Dürig, GG, Art. 2 Abs. 1 Rn. 41; BAG, NZA 2008, 1187 Rn. 20.
29 *Gola/Jaspers*, RDV 2009, 212, 213.
30 BAG, NZA 2008, 1187 Rn. 21, vgl. *Löwisch*, DB 2009, 2782, 2785. Beim Sammeln von Angaben über Beschäftigte ist zudem der Grundsatz der Direkterhebung beim Betroffenen zu beachten, § 4 Abs. 2 BDSG.
31 BVerfG, NJW 2006, 1939 Rn. 88: *„Das Gebot der Verhältnismäßigkeit im engeren Sinn verlangt, dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf."* Vgl. auch *Di Fabio*, in: Maunz-Dürig, GG, Art. 2 Abs. 1 Rn. 41; *Thüsing*, NZA 2009, 865, 867.

den Persönlichkeitsrechten der betroffenen Beschäftigten gegenüberstehen[32]. Die durch die konkrete Maßnahme eintretende Beeinträchtigung der Persönlichkeitsrechte der betroffenen Beschäftigten muss in einem angemessenen Verhältnis zu dem erstrebten Zweck des Datenumgangs stehen[33]. Wenn Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss des Umgangs mit den Daten das Interesse des Arbeitgebers an dem Umgang mit den Daten überwiegen, ist dieser nicht angemessen[34].

Beispiel: Unternehmen dürfen die Einhaltung der Arbeitszeit durch Zeiterfassungssysteme, Stechuhren, Magnetkarten und ähnliche Systeme kontrollieren[35]. Die systematische Erfassung jeder kurzen Pause oder jedes Toilettengangs hingegen wäre unangemessen[36]. Die Erhebung und Auswertung von Daten über Fehlzeiten von Beschäftigten ist nicht nur zum Zweck der Entgeltabrechnung angemessen, sondern auch mit dem Ziel, die Voraussetzungen einer personenbedingten Kündigung zu überprüfen[37]. Hier sind die betroffenen wirtschaftlichen Interessen des Arbeitgebers als schwerwiegender zu bewerten als das Interesse des Beschäftigten am vertraulichen Umgang mit Angaben über seine Fehltage. Die weitere Nutzung dieser Daten, etwa für die Erstellung eines Persönlichkeitsprofils, wäre hingegen nicht angemessen[38].

Um festzustellen, ob die betroffenen Interessen des Beschäftigten oder die des Arbeitgebers höher zu bewerten sind, ist eine Gesamtabwägung der Intensität des Eingriffs und des Gewichts der ihn rechtfertigenden Gründe vorzunehmen[39]. Für die Schwere des Eingriffs ist von Bedeutung, wie viele Personen wie intensiv den Beeinträchtigungen ausgesetzt sind[40].

a) Bewertung der Intensität von Eingriffen

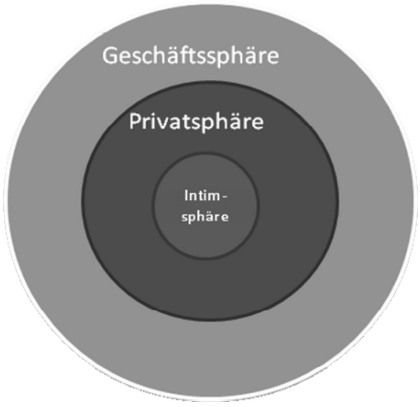
In der betrieblichen Praxis ist es vor allem bei Kontrollmaßnahmen schwierig, deren Erforderlichkeit zu beurteilen. Bei Überwachungsmaßnahmen hängt die Intensität des Eingriffs in die Persönlichkeitsrechte der Beschäftigten von der Art und Dauer der Kontrolle ab. Bei jedem Umgang mit Beschäftigtendaten ist daher vor jeder Maßnahme erst einmal ein klares Bild über das genaue Ausmaß des Eingriffs in Persönlichkeitsrechte der Betroffenen zu gewinnen. Auch hierbei kann die bisherige Rechtsprechung herangezogen werden.

b) Einteilung nach Lebenssphären der betroffenen Beschäftigten

Das Bundesverfassungsgericht hatte bereits im Rahmen der Verwertbarkeit rechtswidrig gewonnener Beweismittel oder der Zulässigkeit staatlicher Kontrollmaßnahmen ähnliche Abwägungen von Persönlichkeitsrechten und Aufklärungsinteressen vorzunehmen; zuletzt im Urteil des 1. Senats zur Vorratsdatenspeicherung[41]. Dabei entwickelten die Richter Grundsätze, die sich auch auf die Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten übertragen lassen[42]. Maßgeblich ist demnach, welchen Lebensbereich die fraglichen Daten betreffen[43]. Es ist zu unterscheiden zwischen Informationen aus dem geschäftlichen oder sozialen Bereich (erste Sphäre), der schlichten Privatsphäre (zweite Sphäre) und der Intimsphäre (dritte Sphäre) der Betroffenen[44] (vgl obenstehende Abbildung).

aa) Geschäftssphäre

Geschäftliche Informationen über seine Beschäftigten wird der Arbeitgeber für einen der in § 32 Abs. 1 S. 1 BDSG genannten Zwecke regelmäßig verwenden dürfen, wenn der Umgang mit den Daten in



geeigneter und erforderlicher Weise geschieht. Voraussetzung ist stets ein im Zusammenhang mit der Beschäftigung stehendes berechtigtes Interesse des Arbeitgebers[45]. Etwa bei beruflichen Fähigkeiten und Erfahrungen sowie zeitlicher Verfügbarkeit liegt ein solches in aller Regel vor[46], da der Umgang mit solchen Daten in der Regel für die Durchführung des Arbeitsverhältnisses erforderlich ist.

Beispiel: Der Vergleich der Eignung von Bewerbern auf der Grundlage von Bewerbungsunterlagen und öffentlich zugänglichen Daten, aber auch die Überprüfung der von Bewerbern genannten Ausbildungsnoten wird in den meisten Fällen als angemessen zu beurteilen sein. Dies gilt auch für den Umgang mit Personaldaten von Arbeitnehmern oder Bewerbern, um deren Eignung für eine bestimmte Aufgabe oder ein Einsatzgebiet zu ermitteln. Nicht angemessen ist hingegen die unbegrenzte Speicherung von Daten von abgelehnten Bewerbern[47].
Unproblematisch sind in aller Regel der auf die Tätigkeit bezogene Umgang mit Stammdaten von Beschäftigten, z. B. Name, Anschrift, Geschlecht, Familienstand, Ausbildung, Eintrittsdatum, Krankenkassenzugehörigkeit usw.[48].

bb) Privatsphäre

Im Rahmen der normalen Personalarbeit ist der Umgang mit Daten, die der Privatsphäre von Beschäftigten entstammen, grundsätzlich nicht angemessen. Freizeitbeschäftigungen, Verwandte, Bekannte,

32 *Schmidt*, RDV 2009, 193, 199: „*Das Interesse des Arbeitgebers wird grundrechtlich von seinem Eigentumsrecht und dem Recht am eingerichteten und ausgeübten Gewerbebetrieb erfasst.*"
33 BAG, NZA 2008, 1187 Rn. 21. Eine solche Wertung enthält auch die dem BDSG zugrunde liegende EG-Datenschutzrichtlinie (RL 95/46/EG) in Art. 7 lit f).
34 Vgl. hierzu die im Wortlaut von § 28 Abs. 1 S. 1 Nr. 2 BDSG und § 32 Abs. 1 S. 2 BDSG zum Ausdruck kommende Wertung des Gesetzgebers.
35 BAG, NZA 1986, 526, 528.
36 *Wellhöner/Byers*, BB 2009, 2310, 2315.
37 *Löwisch*, DB 2009, 2782, 2785. Bei Daten über krankheitsbedingte Abwesenheiten von Beschäftigten handelt es sich um Angaben über deren Gesundheit und damit um besonders geschützte personenbezogene Daten gemäß § 3 Abs. 9 BDSG (sog. sensible Daten). Für den Umgang mit sensiblen Daten gelten strenge Anforderungen. Die Auswertung der krankheitsbedingten Abwesenheitstage im Rahmen einer personenbedingen Kündigung wäre hier gemäß § 28 Abs. 6 Nr. 3 BDSG zur Ausübung rechtlicher Ansprüche des Arbeitgebers erforderlich.
38 *Löwisch*, DB 2009, 2782, 2785. Der Datenumgang zur Erstellung eines Persönlichkeitsprofils würde nicht unter den Erlaubniskatalog des § 28 Abs. 6 BDSG fallen.
39 BAG, NZA 2008, 1187 Rn. 21.
40 BAG, NZA 2008, 1187 Rn. 21.
41 Vergleiche hierzu im Einzelnen *Wybitul*, BB 2010, 889 ff.
42 Vgl. zur Ausstrahlung des Verfassungsrechts bei der Anwendung bzw. Auslegung zivilrechtlicher Normen nach der Theorie der mittelbaren Drittwirkung beim allgemeinen Persönlichkeitsrecht, dem Recht auf informationelle Selbstbestimmung und im Arbeitsrecht: *Di Fabio*, in: Maunz-Dürig, GG, Art. 2 Abs. 1 Rn. 138 ff.
43 Sog. Sphärentheorie, vgl. *Di Fabio*, in: Maunz-Dürig, GG, Art. 2 Abs. 1 Rn. 41.
44 BVerfGE 34, 238, 245 ff.
45 Vgl. BAG, DB 2003, 396; zusammenfassend *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 32 Rn. 16.
46 Vgl. *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 32 Rn. 19.
47 Geht es hingegen allein um eine statistische Auswertung dieser Daten, so sollte der Arbeitgeber eine Verarbeitung nach vorheriger „Entpersonalisierung" durch Anonymisierung prüfen. Denn aggregierte oder anonymisierte Daten schützt das BDSG nicht, *Gola/Jaspers*, Das novellierte BDSG im Überblick, 5. Aufl. 2010, S. 19.
48 *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 32 Rn. 68.

Hobbies, Ess- oder Trinkgewohnheiten seiner Beschäftigten gehen den Arbeitgeber in der Regel wenig an[49]. Etwas anderes gilt allerdings, wenn ein berechtigtes Interesse des Arbeitgebers an der fraglichen Information vorliegt. Dies ist dann der Fall, wenn sich die Information aus dem Privatleben auf das Beschäftigungsverhältnis auswirken kann.

Beispiel: Wenn ein Beschäftigter wegen zu schneller Fahrt oder Trunkenheit am Steuer seine Fahrerlaubnis verliert, ist dies in den allermeisten Fällen nicht Sache des Arbeitgebers. Anders ist dies bei einem als Kraftfahrer angestellten Beschäftigten[50]. Hier wird der Arbeitgeber in der Regel ein berechtigtes Interesse haben, Überprüfungen oder Nachforschungen anzustellen. Ebenso hat ein Arbeitgeber ein berechtigtes Interesse, bei der Einstellung eines Jugendpflegers nach Vorstrafen wegen Sexualdelikten oder bei derjenigen eines Kassierers nach Vermögensdelikten zu forschen[51].
Bei konkreten Verdachtsmomenten, die auf Vertragsverstöße eines Arbeitnehmers hindeuten, ist der Arbeitgeber auch berechtigt, einen Detektiv mit der Aufklärung des Vorgangs zu beauftragen. Die Ermittlungen durch Detekteien berühren in der Praxis fast ausnahmslos Daten aus der Privatsphäre der Betroffenen.

cc) Intimsphäre (Kernbereich privater Lebensgestaltung)

Die Menschenwürde schützt einen Kernbereich vertraulicher Kommunikation[52]. Arbeitgebern ist der Umgang mit Daten grundsätzlich verwehrt, die der Intimsphäre ihrer Beschäftigen entstammen oder diese betreffen. Dies gilt etwa für die Auswertung der E-Mail-Korrespondenz zwischen Eheleuten oder Familienmitgliedern[53] oder das Mithören von Telefonaten zwischen diesen[54], tagebuchartige Aufzeichnungen des Arbeitnehmers auf dem Firmenlaptop, Informationen über das Sexualleben, mittels Gentests gewonnene Daten usw. In diesen Fällen werden Eingriffe in die Persönlichkeitsrechte der Betroffenen allenfalls unter absolut außergewöhnlichen Umständen und zum Schutz elementarer Arbeitgeberinteressen angemessen sein[55]. Eine Hilfe bei der Frage, ob die besonders schutzwürdige Intimsphäre der betroffenen Beschäftigten berührt ist, gibt § 100c Abs. 4 S. 2 StPO: „*Gespräche in Betriebs- oder Geschäftsräumen sind in der Regel nicht dem Kernbereich privater Lebensgestaltung zuzurechnen.*"
Berührt eine Kontrollmaßnahme möglicherweise auch die Intimsphäre von Beschäftigten, so ist besonders streng darauf zu achten, dass dem Verhältnismäßigkeitsgrundsatz auch durch flankierende Maßnahmen Rechnung getragen wird, etwa durch möglichst weitgehende Anonymisierung oder Pseudonymisierung, durch vorherige Ausfilterung von Informationen, die nicht erforderlich sind. Zudem muss sichergestellt sein, dass sich die Anzahl und Intensität solcher Eingriffe auf das für den Zweck des Datenumgangs absolut nötige Maß beschränkt[56]. Auch hier können strafprozessuale Vorgaben des Gesetzgebers zur Orientierung herangezogen werden. Danach sind Kontrollmaßnahmen unverzüglich abzubrechen, wenn Anhaltspunkte dafür auftreten, dass Äußerungen erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind; Aufzeichnungen über solche Äußerungen sind unverzüglich zu löschen[57].
Der Umgang mit solchen Daten wird in aller Regel nur dann angemessen sein, wenn der Eingriff in die Persönlichkeitsrechte der Betroffenen nur eine sehr geringe Intensität hat oder die Erhebung, Verarbeitung oder Nutzung absolut nötig ist, um elementare Interessen des Arbeitgebers zu verwirklichen. Dies kann beispielweise bei internen Ermittlungen, etwa wegen konkreten Kartellverstößen oder Korruptionsvorwürfen der Fall sein[58].

PRAXISTIPP: Sofern möglich, ist bei Eingriffen in die Intimsphäre Beschäftigter zu versuchen, den Umgang mit den Daten nicht allein auf § 32 BDSG zu stützen, sondern von den Betroffenen Einwilligungen in den Umgang mit ihren Daten einzuholen. Zwar sind die formellen und inhaltlichen Voraussetzungen an wirksame Einwilligungen nach § 4a BDSG sehr hoch. Aber selbst das Vorliegen einer lediglich aus formellen Gründen nicht als ausreichend zu beurteilenden Einwilligung kann im Rahmen der Angemessenheit relevant sein. Denn der Betroffene hat immerhin zu verstehen gegeben, dass er keine grundsätzlichen Vorbehalte gegen den Eingriff in seine Intimsphäre hat.

V. Umsetzung des Verhältnismäßigkeitsgrundsatzes in der betrieblichen Praxis

Die Beantwortung der Frage nach der Zulässigkeit des Umgangs mit Beschäftigtendaten bei der Personalarbeit lässt sich durch einige Maßnahmen deutlich vereinfachen. Auf einer ersten Stufe ist der Zweck der Datenerhebung genau festzulegen. Denn erst die genaue Bestimmung des Zwecks der Datenerhebung ermöglicht die spätere Feststellung, ob der jeweilige Umgang mit den Beschäftigtendaten zur Erreichung dieses Zwecks geeignet, erforderlich und angemessen ist.

1. Genaue Festlegung der konkreten Zwecke der beabsichtigen Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten

Gemäß § 28 Abs. 1 S. 2 BDSG sind bei der Erhebung personenbezogener Daten die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen[59]. Diese Regelung gilt auch im Rahmen von Beschäftigungsverhältnissen[60]. Daher ist die Speicherung von Beschäftigtendaten auf Vorrat ausgeschlossen, denn dabei fehlt es an der nötigen konkreten Festlegung des Zwecks[61]. Bei der Erhebung von Daten ist auch der so genannte Grundsatz der Direkterhebung zu beachten[62]. Danach müssen personenbezogene Daten nach Möglichkeit direkt beim Betroffenen erhoben werden. Dies gilt nur dann nicht, wenn eine der in § 4 Abs. 2 BDSG genannten Ausnahmen vorliegt, etwa weil eine Erhebung beim Betroffenen selbst einen unverhältnismäßigen Aufwand erfordern würde. Werden Daten beim Betroffenen direkt erhoben, so ist er grundsätzlich[63] auch über den Zweck der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten zu informieren[64].

49 *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 32 Rn. 17.
50 BAG, AP Nr. 74 zu § 611 BGB Haftung des Arbeitnehmers.
51 *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 32 Rn. 35.
52 BVerfGE 109, 279, 313; BVerfG, NJW 2010, 287, 288.
53 Vgl. BVerfG, NJW 2010, 287, 288.
54 In diesen Fällen ist stets auch an das Post- bzw. Fernmeldegeheimnis zu denken, dessen Verletzung strafbewehrt ist.
55 Anders *Schmidt*, RDV 2009, 193, 199, der von einem absoluten Verbot der Nutzung von Beschäftigtendaten ausgeht. Dieser Standpunkt ist vertretbar, lässt aber außer Acht, dass bei Kontrollmaßnahmen regelmäßig auch unerwünschte Informationen anfallen, die gegebenenfalls der Intimsphäre der Beschäftigten entstammen. Hört etwa ein Vorgesetzter zufällig ein Gespräch mit, in dem der Beschäftigte von einem sexuellen Abenteuer berichtet, das sich dieser mit veruntreuten Geldern des Arbeitgebers „geleistet" hat, so wird er diese Information auch aus datenschutzrechtlicher Sicht nutzen dürfen. In der Praxis interner Ermittlungen sind solche unerwünschten Zufallsfunde aus der Intimsphäre der Betroffenen deutlich häufiger, als es der Laie annehmen würde.
56 Erfahrungsgemäß sind Angaben, die der Intimsphäre von Betroffenen entstammen, oft auch sensible Daten i. S. v. § 3 Abs. 9 BDSG. In diesem Falle ist zu prüfen, ob der Umgang mit den sensiblen Daten nach § 28 Abs. 6 BDSG erlaubt ist.
57 § 100c Abs. 5 S. 1 und 2 StPO.
58 Vgl. *Salvenmoser/Hauschka*, NJW 2010, 331, 333.
59 Allerdings gibt es zu dieser Vorschrift eine Reihe von Ausnahmen, vgl. § 28 Abs. 2, 3 und 8 BDSG.
60 Vgl. *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 38 Rn. 63.
61 *Däubler*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2009, § 32 Rn. 134.
62 § 4 Abs. 2 BDSG.
63 Dies gilt nicht, wenn er bereits auf andere Weise Kenntnis erlangt hat, § 4 Abs. 3 S. 1 BDSG.
64 § 4 Abs. 3 S. 1 Nr. 2 BDSG.

2. Prüfung der Möglichkeiten zur Umsetzung des Zwecks des Datenumgangs

Auf einer zweiten Stufe sind dann die zur Erreichung des Zwecks zulässigen Möglichkeiten zu prüfen. Führen mehrere gleich geeignete Vorgehensweisen zu dem gewählten Zweck, ist die mildeste zu wählen, also diejenige, die am wenigsten intensiv in Persönlichkeitsrechte der betroffenen Beschäftigten eingreift. Der Schwerpunkt der Frage nach der Erforderlichkeit wird in aller Regel bei der Abwägung der betroffenen Interessen, also bei der Prüfung der Angemessenheit liegen.

Hier sollte der Arbeitgeber zunächst prüfen, ob der geplante Datenumgang das normale geschäftliche Umfeld der betroffenen Arbeitnehmer, deren Privatsphäre oder sogar deren Intimsphäre betrifft. Auch die zeitliche Dauer und die Anzahl der betroffenen Arbeitnehmer sind maßgeblich. Je intensiver ein Eingriff sich auf die Persönlichkeitsrechte auswirkt, desto wichtiger muss der vom Arbeitgeber bei der Erhebung, Verarbeitung oder Nutzung der Daten verfolgte Zweck sein.

3. Praxishilfe: Checkliste zur Umsetzung der Anforderungen des BDSG bei der Personalarbeit

// BB-Checkliste

- Existieren Spezialgesetze[65], die den Umgang mit den fraglichen Daten erlauben[66]? In diesem Fall ist eine Prüfung der Voraussetzungen von § 32 BDSG nicht erforderlich.
- Sind alle Möglichkeiten zum Umgang mit anonymisierten (oder wo dies nicht zweckmäßig ist, pseudonymisierten) Daten ausgeschöpft[67]?
- Ist die Prüfung der Zulässigkeit kritischer Maßnahmen (insbesondere die erforderliche Interessenabwägung) hinreichend dokumentiert? Es ist sehr ratsam, alle Maßnahmen schriftlich festzuhalten, mit denen sichergestellt wird, dass die Interessen der Betroffenen nur in möglichst geringem Umfang berührt werden[68].
- Ist sichergestellt, dass von einer datenschutzrechtlich relevanten Maßnahme ausschließlich Beschäftigte betroffen sind, die in engem Zusammenhang mit dem erstrebten Zweck der Maßnahme stehen[69]? Ist der Datenumgang auf den für den erstrebten Zweck maßgeblichen Bereich des Unternehmens beschränkt[70]? Sind Stichproben ausreichend oder ist eine flächendeckende Maßnahme nötig?
- Ist der Umgang mit den Beschäftigtendaten zeitlich hinreichend eingegrenzt[71]? Beispielsweise sind die bei einer Überwachung anfallenden Daten umgehend zu löschen, sobald sie nicht mehr gebraucht werden[72].
- Ist sichergestellt, dass bei Verhaltenskontrollen intensive Eingriffe in Persönlichkeitsrechte (z. B. Videokontrollen) nicht verdachtsunabhängig vorgenommen werden, sondern stets Reaktion auf konkrete Anhaltspunkte sind?
- Besteht die Möglichkeit, einzelne Maßnahmen durch Einwilligungen der betroffenen Beschäftigten nach § 4a BDSG zu legitimieren[73]?
- Sind alle Möglichkeiten zur Überprüfung der rechtlichen Zulässigkeit kritischer Maßnahmen ausgeschöpft? Ein praktikabler Weg hierfür ist oft eine direkte Kontaktaufnahme mit der zuständigen Datenschutz-Aufsichtsbehörde. Diese ist gesetzlich verpflichtet, sowohl die verantwortliche Stelle als auch deren Datenschutzbeauftragten zu unterstützen und beraten[74].
- Sind alle Optionen genutzt, Fragen der datenschutzrechtlichen Zulässigkeit von Maßnahmen durch den Abschluss von Betriebsvereinbarungen[75] zu klären? Dies ist in der betrieblichen Praxis einer der effektivsten Wege, um Grauzonen auszuleuchten.

VI. Ergebnis

Mit dem neuen § 32 BDSG ist dem Gesetzgeber sicherlich kein großer Wurf gelungen. Die Regelung birgt viele Unklarheiten und erschwert Personalern und Compliance-Verantwortlichen die Erfüllung ihrer Aufgaben. Werden allerdings die vorstehend dargelegten Grundsätze systematisch und konsequent angewandt, so kann auch diese wenig geglückte Vorschrift so konkret ausgelegt werden, dass sie ein gewisses Maß an Planbarkeit und Vorhersehbarkeit bietet. Die Kriterien lassen sich auf § 32 Abs. 1 S. 1 BDSG („für Zwecke des Beschäftigungsverhältnisses") ebenso wie auf § 32 Abs. 1 S. 2 BDSG („zur Aufdeckung von Straftaten") anwenden. Das Merkmal der Erforderlichkeit verwendet der Gesetzgeber noch in einer Vielzahl weiterer Vorschriften des BDSG[76]. Auch hierauf lassen sich die dargestellten Überlegungen grundsätzlich übertragen.

Es steht zu hoffen, dass die Arbeitsgerichte diese Maßstäbe möglichst schnell umsetzen und Arbeitnehmern und Arbeitgebern eine verlässliche Rechtsprechung zum Umgang mit § 32 BDSG an die Hand geben.

// Autor

Tim Wybitul berät Wirtschaftsunternehmen bei Datenschutz, Compliance und internen Ermittlungen. Unter anderem leitet Herr *Wybitul* seit geraumer Zeit ein Team von Anwälten, das eine Schweizer Großbank im Rahmen strafrechtlicher Untersuchungen der US-Behörden SEC, DOJ und IRS unterstützt.

65 Das BetrVG beispielsweise regelt umfangreiche Informationspflichten des Arbeitgebers gegenüber dem Betriebsrat. Eine Weitergabe von Arbeitnehmerdaten wird i. d. R. keine Übermittlung (§ 3 Abs. 4 Nr. 3 BDSG) an eine andere verantwortliche Stelle, sondern eine Nutzung (§ 3 Abs. 5 BDSG) darstellen. Die Weitergabe der in § 99 Abs. 1 BetrVG genannten Informationen über betroffene Arbeitnehmer im Rahmen einer personellen Einzelmaßnahme ist durch diese Rechtsnorm auch datenschutzrechtlich erlaubt.

66 Gleicht etwa ein Finanzinstitut Kontodaten, die im Zusammenhang mit verdächtigen Transaktionen stehen, mit Kontodaten von bei diesen Transaktionen besonders exponierten Mitarbeitern ab, so kann dieser Datenumgang gegebenenfalls auf § 25c Abs. 2 KWG gestützt werden: *„Kreditinstitute haben angemessene Datenverarbeitungssysteme zu betreiben und zu aktualisieren, mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen, die […] als zweifelhaft oder ungewöhnlich anzusehen sind. […] Die Kreditinstitute dürfen personenbezogene Daten erheben, verarbeiten und nutzen, soweit dies zur Erfüllung dieser Pflicht erforderlich ist."*

67 Vgl. *Schmidt*, RDV 2009, 193, 198.

68 Zwar kann nicht ausgeschlossen werden, dass die zuständige Datenschutz-Aufsichtsbehörde später bei einer Überprüfung der Zulässigkeit der geplanten Datentransfers zu einem abweichenden Ergebnis gelangt. In einem solchen Fall dürften die negativen Folgen aber zumindest dann gering sein, wenn die verantwortliche Stelle schlüssig darlegen kann, warum sie welche Schritte unternommen hat und auf welcher Grundlage sie davon ausging, in rechtlich zulässiger Weise zu handeln.

69 Vgl. *Barton*, RDV 2009, 200, 201, der an dieser Stelle auch sehr zutreffend das Dilemma beschreibt, in dem sich Unternehmen befinden, die einerseits den Compliance-Anforderungen genügen müssen, die von dem Gesetzgeber und den Gerichten an Unternehmen gestellt werden – und sich andererseits einem wenig konkreten BDSG ausgesetzt sehen, wenn sie entsprechende Kontrollmaßnahmen ergreifen.

70 Diese Erwägung ergibt sich aus dem Verhältnismäßigkeitsgrundsatz und ist vom Gesetzgeber auch außerhalb des Datenschutzrechts aufgegriffen worden, z. B. § 100c Abs. 3 StPO.

71 Vgl. Art. 6 Abs. 1 lit. e) RL 95/46/EG.

72 Vgl. hierzu den ausgesprochen hilfreichen Beitrag von *Kock/Francke*, NZA 2009, 646, 648.

73 Zwar wird die Einwilligung im Arbeitsverhältnis im Hinblick auf die erforderliche Freiwilligkeit der Einwilligung teilweise sehr kritisch gesehen, vgl. hierzu *Schmidt*, RDV 2009, 193, 194. Allerdings hat der Gesetzgeber in der Gesetzesbegründung des BDSG 2009 die bislang streitige Frage, ob eine Einwilligung im Arbeitsverhältnis nur unter besonderen Anforderungen möglich ist, wohl nun eindeutig geklärt. In der Gesetzesbegründung (BT-Drs 16/13657, S. 20) heißt es hierzu: *„Auch eine Datenerhebung oder -verwendung auf der Grundlage einer freiwillig erklärten Einwilligung des Beschäftigten (§ 4a des Bundesdatenschutzgesetzes, § 22 des Kunsturhebergesetzes) wird durch § 32 nicht ausgeschlossen."* Würde der Gesetzgeber davon ausgehen, dass eine Einwilligung im Arbeitsverhältnis tatsächlich nur unter engen Voraussetzungen möglich wäre, so hätte er das bei dieser Gelegenheit sicher angesprochen. Nachdem er sich in diesem Zusammenhang sogar mit der schwerlich zentralen Rechtsnorm des § 22 Kunsturhebergesetz befasst hat, ist nicht anzunehmen, dass der Gesetzgeber diese Kernfrage des Beschäftigtendatenschutzes schlichtweg übersehen hat.

74 §§ 38 Abs. 1 S. 2, 4g Abs. 1 S. 2, 4d Abs. 6 S. 3 BDSG.

75 Betriebsvereinbarungen sind als Erlaubnisnormen nach § 4 Abs. 1 BDSG anerkannt. Sie können zwar keine unverhältnismäßigen Eingriffe in die Persönlichkeitsrechte von Arbeitnehmern rechtfertigen, sind aber erfahrungsgemäß ein sehr praktisches Mittel, um Unsicherheiten in der konkreten Umsetzung des BDSG auszuschließen, vgl. auch *Kock/Francke*, NZA 2009, 646, 649.

76 Z. B. § 28 Abs. 1 S. 1 Nr. 1 und 2, Abs. 2 Nr. 2 und 3, Abs. 6 Nr. 3 und 4, Abs. 7, Abs. 8, Abs. 9, § 28a Abs. 1, § 4 2. S. 2 Nr. 2a, § 4c Abs. 1 Nr. 1, 2, 3 und 4.