Die Rechte der Beschäftigten im novellierten Bundesdatenschutzgesetz

Die Rechte der Beschäftigten gewinnen sowohl durch die Änderungen des Datenschutzrechts als auch durch die zunehmende Verarbeitung personenbezogener Daten der Beschäftigten an Bedeutung. Denn jede Person – ob als Beschäftigter, Bürger, Kunde, Klient – sollte die Möglichkeit haben, wissen zu können, welche Daten über ihn verarbeitet werden. Dieses hat bereits 1983 das Bundesverfassungsgericht (BVerfG) im sogenannten Volkszählungsurteil festgestellt.

Da in der Praxis von den Rechten der Beschäftigten auf Information, Benachrichtigung, Auskunft oder Korrektur von Daten wenig Gebrauch gemacht wird und es Neuerungen im Bundesdatenschutzgesetz (BDSG) gibt, sollen nachfolgend die Rechte näher betrachtet werden. Für die Personalräte ist dieses von Bedeutung, da sie die Einhaltung bestehender Gesetze (in diesem Fall das BDSG) auf Einhaltung zu überwachen zu haben. Zudem sollte die Interessenvertretung prüfen, inwieweit diese im BDSG verankerten Rechte in Dienstvereinbarungen ihren Niederschlag finden sollten. Wenn Dienstvereinbarungen bestehen sollte geprüft werden, ob hier vor dem Hintergrund der Novellierung des BDSG Anpassungen vorzunehmen sind.

1. Datenschutz im öffentlichen Dienst

Sollen personenbezogene der Beschäftigten erhoben, verarbeitet oder genutzt werden, wird in der Regel die Zulässigkeit der Datenverarbeitung aus den Datenschutzgesetzen herzuleiten sein. Auf Grund der verschiedenen gesetzlichen Regelungen zum Datenschutz, wie dem BDSG[1] und daneben bestehenden Datenschutzgesetzen[2] der Länder herrscht insbesondere für die Beschäftigten im öffentlichen Dienst eine gewisse Unübersichtlichkeit und somit auch Unklarheit, welche gesetzlichen Vorgaben in der Praxis anzuwenden sind. Nimmt man das BDSG zur Hand so nennt das Gesetz in § 1 unter „Zweck und Anwendungsbereich" des Gesetzes folgende Adressaten:

- öffentliche Stellen des Bundes,
- öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und
- nicht-öffentliche Stellen.

Für die **öffentlichen Stellen des Bundes** finden der erste, zweite, vierte, fünfte und sechste Abschnitt des BDSG Anwendung. Für öffentliche Stellen des Bundes gilt jedoch an Stelle des zweiten Abschnitts der dritte Abschnitt und zwar dann, wenn diese Stellen als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Das heißt, diese Stellen werden datenschutzrechtlich den Privatbetrieben gleichgestellt. Da alle Bundesländer eigene Datenschutzgesetze erlassen haben, ist für **öffentliche Stellen der Länder** das jeweilige Landesdatenschutzgesetz anzuwenden. Für die sogenannten **nicht-öffentlichen Stellen**, wozu Privatbetriebe in jeder Rechtsform, Vereine und Stiftungen gehören, gilt der erste, dritte, vierte, fünfte und sechste Abschnitt des BDSG.

Auf die weiteren Ausnahmefälle soll nicht weiter eingegangen werden, da es schon vor dem Hintergrund des Dargestellten deutlich wird, das ein eigenständiges Arbeitnehmer-Datenschutzgesetzes[3] längst überfällig ist.

Damit Beschäftigte im öffentlichen Dienst (des Bundes) und die Beschäftigten in der Privatwirtschaft (nicht-öffentlicher Bereich) unter datenschutzrechtlichen Gesichtspunkten gleichbehandelt werden, verweist § 12 Abs. 4 BDSG in Bezug auf den Beschäftigten-Datenschutz auf den für die Beschäftigten der Privatbetriebe geltenden dritten Abschnitt des BDSG. Nach § 12 Abs. 4 BDSG sind auf die Verarbeitung personenbezogener Daten für frühere, bestehende oder zukünftige arbeitsrechtliche Rechtsverhältnisse an Stelle der §§ 13 bis 16[4], 19 bis 20[5] der § 28 Abs. 1 und 3 Nr. 1[6] sowie die §§ 33 – 35 BDSG[7] anzuwenden. Das heißt, dass die in dieser Abhandlung erörterten Rechte der Beschäftigten sowohl für den öffentlichen Bereich des Bundes als auch für den nicht-öffentlichen Bereich gelten. Für den öffentlichen Bereich der Länder sind die aufgezeigten Rechte in gleicher Weise vorhanden.

2. Transparenz der Datenverarbeitung

Gerade mit der Novellierung des BDSG, der zunehmenden Datenverarbeitung im Arbeitsleben und im öffentlichen Leben sind die Aussagen des BVerfG zum Datenschutz (Schutz der Persönlichkeitsrechte) von zentraler Bedeutung. Das BVerfG hat in seinem Urteil[8] vom 15. 12. 1983 aus Art. 1 Abs. 1 und Art. 2 Abs. 1 Grundgesetz ein Recht jedes einzelnen auf **informationelle Selbstbestimmung** abgeleitet. In der Erkenntnis der mit der modernen Datenverarbeitung verbundenen Gefahren für die Betroffenen führt

1) Bundesdatenschutzgesetz vom 20. Dezember 1990 (BGBl. I. S. 2954), zuletzt geändert durch Art. 1 des Gesetzes vom 18. 5. 2001 (BGBl. I S. 904).

2) Die Landesdatenschutzgesetze sind nach Vorgabe der EG-Datenschutzrichtlinie zum goßen Teil novelliert worden. Dieses wird aus der Tabelle zu diesem Artikel deutlich.

3) Die Bundesregierung will bis 2002 ein seperates Arbeitnehmer-Datenschutzgesetz auf den Weg bringen; vgl. hierzu Handesblatt v. 16. 10. 2000, S. 5, Tinnefeld/Viethen, Arbeitnehmerdatenschutz und Internet-Ökonomie, NZA 2000, S. 977 ff..

4) Diese Paragraphen enthalten die Zulässigkeit der Datenerhebung (§ 13 BDSG), Datenspeicherung, -veränderung und -nutzung (§ 14 BDSG) und Datenübermittlung (§§ 15 und 17 BDSG).

5) Diese Paragraphen enthalten Auskunftrecht des Betroffenen (§ 19 BDSG) und die Rechte auf Berichtigung, Löschung udn Sperrung von Daten und das Widerspruchsrecht (§ 20 BDSG).

6) § 28 BDSG enhält die Zulässigkeitsvoraussetzungen für die Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke.

7) §§ 33–35 BDSG enthalten die zentralen Rechte der Beschäftigen auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung, die Ggenstand dieser Abhandlung sind.

8) Vgl. BVerfG, Urteil v. 15. 12. 1983, NJW 1984, S. 419 ff.

das Gericht aus: „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus." Zudem stellt das Gericht das Recht einzelnen heraus, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden." Das Recht auf informationelle Selbstbestimmung ist jedoch nicht „schrankenlos". Einschränkungen dieses Rechts bedürfen aber einer gesetzlichen Grundlage. Anders ausgedrückt bedeutet dies, dass jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur auf der Basis eines Gesetzes erfolgen darf.

Für die Existenz und Ausübung des Rechts auf informationelle Selbstbestimmung bildet Transparenz über die Datenverarbeitung eine wesentliche Voraussetzung[9]. Das Bundesverfassungsgericht führt dazu aus: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt sein, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen, wer was bei welcher Gelegenheit über sie weiß."[10] Transparenz der Datenverarbeitung gehört somit zu den verfassungsrechtlich gewährleisteten Grundpositionen der Betroffenen (Beschäftigten). Zur möglichen Transparenz kann u.a. die verstärkte Nutzung der in den §§ 33 – 35 BDSG verankerten Rechte der Betroffenen beitragen.

3. Rechte und Pflichten der Betroffenen im Einzelnen

Das BDSG enthält eine Reihe von Rechtsansprüchen der Betroffenen. Dies sind die Rechte auf

- Unabdingbarkeit der Rechte — § 6 BDSG
- Information — § 4 Abs. 3 BDSG
- Unterrichtung — § 6c BDSG
- Benachrichtigung — § 33 BDSG
- Auskunft — § 34 Abs. 1 BDSG
- Berichtigung — § 35 Abs. 1 BDSG
- Löschung — § 35 Abs. 2 BDSG
- Sperrung — § 35 Abs. 4 BDSG
- Recht auf Widerspruch — § 35 Abs. 5 BDSG
- Verpflichtung auf das Datengeheimnis — § 5 BDSG
- Schadensersatz — §§ 7 und 8 BDSG

4. Unabdingbarkeit der Rechte

Die Rechte nach §§ 34 und 35 BDSG sind gemäß § 6 Abs. 1 BDSG unabdingbar und können durch ein Rechtsgeschäft weder ausgeschlossen noch beschränkt werden. Demzufolge sind Vereinbarungen, die diese Rechte ganz oder teilweise einschränken, unwirksam. Dieses gilt sowohl für den Abschluss von Einzelverträgen als auch für den Abschluss von Dienstvereinbarungen. Da das Recht auf informationelle Selbstbestimmung (Daten-Transparenz) ein bedeutendes Rechtsgut ist, ist es nur konsequent, dass durch § 6 BDSG die Vertragsfreiheit eingeschränkt wird. Denn insbesondere in Abhängigkeitsverhältnissen, wie in Arbeitsverhältnissen, ist der schwächere Vertragspartner (Arbeitnehmer) eher bereit, auf seine Rechte zu verzichten[11].

5. Informationsrecht

In § 4 Abs. 3 BDSG ist eine Neuregelung bei der Erhebung von Daten enthalten. Zum einen ist das Prinzip der Direkterhebung und zum anderen ein Informationsrecht verankert. Zudem muss die verarbeitende Stelle zum Zeitpunkt der Erhebung eine konkrete Festlegung der Verarbeitungszwecke vornehmen. So ist im Falle der Direkterhebung (Erhebung beim Betroffenen) der Beschäftigte (der Betroffene) von der verantwortlichen Stelle über folgenden Aspekte zu unterrichten:

- die Identität der verantwortlichen Stelle,
- die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
- die Kategorien von Empfängern, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung rechnen muss.

Eine entsprechende Information muss nicht erfolgen, wenn der Betroffene auf andere Weise Kenntnis erlangt.

6. Recht auf Unterrichtung bei mobilen Speichermedien

Das novellierte BDSG enthält eine Regelung zu mobilen Speicher- und Verarbeitungsmedien. Dieses sind Datenträger

- die an den Betroffenen ausgegeben werden,
- auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
- bei denen der Betroffene diese Verarbeitung durch den Gebrauch des Mediums beeinflussen kann (§ 3 Abs. 10 BDSG).

Erfasst vom BDSG werden also Medien, auf denen personenbezogene Daten über die reine Speicherung hinaus automatisiert verarbeitet werden können. Dieses können z. B. Chipkarten sein, die mit einem Prozessorchip ausgestattet sind. Bloße Speichermedien wie CDs oder Magnetkarten werden vom BDSG nicht erfasst.

Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder Verfahren zur automatisierten Verarbeitung auf diese Medium aufbringt, muss den Betroffenen unterrichten

- über die Identität und Anschrift der Stelle,
- in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden Daten,
- darüber, wie er seine Rechte auf Auskunft, Berichtigung, Löschung und Sperrung ausüben kann,
- über die bei Verlust und Zerstörung zu treffenden Maßnahmen (§ 6c Abs. 1 BDSG).

9) Vgl. Däubler, Individualrechte des Arbeitnehmers nach dem neuen BDSG. Computer und Recht 1991, S. 476; Gola/Schomerus, Bundesdatenschutzgesetz, 6. Aufl., § 33 Anm. 1.1; Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum Bundesdatenschutzgesetz, 4. Aufl., § 33 Rn. 1.

10) Vgl. BVerfG, Urteil v. 15. 12. 1983, NJW 1984, S. 419.

11) Vgl. Däubler (Fn. 9), S. 482.

Zusätzlich hat die verantwortliche Stelle dafür Sorge zu tragen, das die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräten in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen. D.h. dass entsprechende Lesegeräte aufgestellt werden müssen, an denen der Betroffene die über ihn gespeicherten personenbezogenen Daten einsehen und ausdrucken kann.

Kommunikationsvorgänge, die auf dem Verarbeitungs- und Speichermedium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein (§ 6c Abs. 3 BDSG). Damit soll sichergestellt werden, dass Verarbeitungen nicht vom Betroffenen unbemerkt, z. B. durch Vorbeigehen an einem Terminal, ausgelöst werden.

7. Benachrichtigung des Beschäftigten

7.1 Gesetzliche Vorgabe

Werden erstmals personenbezogene Daten ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene gemäß § 33 Abs. 1 BDSG

- von der Speicherung selbst,
- der Art der gespeicherten Daten,
- der Zweckbestimmung der Erhebung, Verarbeitung und Nutzung und
- der Identität der verantwortlichen Stelle zu benachrichtigen.

Eine Benachrichtigung hat zu erfolgen, wenn über einen einzelnen Daten gespeichert werden, zu dessen Person bisher nichts gespeichert wurde. Werden jedoch im Laufe eines Beschäftigungsverhältnisses zusätzliche Daten, z. B. weitreichende Qualifikationsdaten zur Personalplanung, gespeichert, wird zusätzlich eine Benachrichtigung erfolgen müssen. Dies ergibt sich aus der Verpflichtung gemäß § 33 Abs. 1 BDSG, dass auch über die Art der Daten zu benachrichtigen ist[12]. „Andernfalls würde sich das Ziel der Benachrichtigung in sein Gegenteil verkehren, statt Transparenz hinsichtlich der über ihn gespeicherten Daten zu erhalten, würde der Betroffene ggf. in der irrigen Meinung gehalten, dass nur für ihn wenig sensible Daten gespeichert seien, und deshalb von seinem Auskunftsrecht auch keinen Gebrauch machen, während inzwischen durch Änderung der gespeicherten Datenarten sein Persönlichkeitsrecht erheblich tangierende Verarbeitungen stattfinden."[13] Im BDSG sind keine Fristen für die Benachrichtigung enthalten. Nach allgemeiner Auffassung wird eine Benachrichtigung, die unverzüglich (§ 121 BGB), d. h., ohne schuldhaftes Zögern, nach erstmaliger Speicherung zu erfolgen hat, spätestens zwei bis vier Wochen nach erstmaliger Speicherung dem Betroffenen „zugehen" müssen[14]. Das Gesetz schreibt für die Benachrichtigung keine bestimmte Form vor. Sie liegt im Ermessen der verantwortliche Stelle und kann mündlich, telefonisch oder schriftlich erfolgen[15]. Allerdings sollte aus Beweissicherungsgründen vor dem Hintergrund der Vergänglichkeit des gesprochenen Wortes die Schriftform gewählt werden. Damit kann sich die verantwortliche Stelle gegen mögliche Vorwürfe absichern, sie habe die Benachrichtigung unterlassen und damit eine Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 8 BDSG begangen[16].

7.2 Ausnahmen von der Benachrichtigung

§ 33 Abs. 2 BDSG sieht eine Reihe von Ausnahmen von der Benachrichtigungspflicht vor. Die **Ausnahmetatbestände** sind eng und im Zweifel zugunsten der Betroffenen und damit auch zugunsten der Benachrichtigungspflicht zu interpretieren[17].

Erlangung der Kenntnisse von der Speicherung auf andere Weise

Nach § 33 Abs. 2 Nr. 1 BDSG besteht eine Pflicht zur Benachrichtigung nicht, wenn „der Betroffene auf andere Weise Kenntnis von der Speicherung und Übermittlung erlangt hat". In der Praxis kommt dieser Ausnahmeregelung große Bedeutung zu, da hieraus abgeleitet wird, dass in Arbeitsverhältnissen eine Benachrichtigung generell unterbleiben kann[18]. Um der Benachrichtigungspflicht Genüge zu tun, reicht jedoch die reine Möglichkeit der Kenntniserlangung durch den Betroffenen nicht aus; vielmehr muss er diese Kenntnis auch tatsächlich erlangt haben[19]. Bestehen für den Beschäftigten keine erkennbaren Anhaltspunkte, muss er nicht mit einer Datenverarbeitung rechnen.

Hat die verantwortliche Stelle den Betroffenen bei der Erhebung informiert (§ 4 Abs. 3 BDSG), muss keine weitere Benachrichtigung erfolgen. Bei einem Bewerber wird eine Kenntnis von der Speicherung bereits angenommen, wenn dieser einen Personalfragebogen ausgefüllt hat bzw. wenn ein entsprechender Fragebogen auf computerlesbarem Papier gedruckt ist[20]. Es kann jedoch erst dann von einer Kenntniserlangung nach § 33 Abs. 2 Nr. 1 BDSG ausgegangen werden, wenn bspw. auf dem Fragebogen ein Vermerk wie „Bitte wegen Computererfassung leserlich schreiben" aufgedruckt ist[21]. Eine Kenntniserlangung liegt jedoch in der Regel demjenigen Beschäftigten vor, der eine Einwilligungserklärung gemäß § 4 BDSG unterschrieben hat. Dass bei bestehenden Arbeitsverhältnissen grundsätzlich davon ausgegangen werden kann, dass ein Arbeitnehmer Kenntnis über die Personaldatenverarbeitung beim Arbeitgeber hat[22], vermag jedoch vor dem Hintergrund des Rechts auf informationelle Selbstbestimmung und der damit einhergehenden Forderung nach Datentransparenz nicht zu überzeugen.

Gesetzliche Aufbewahrungsfristen/Datenschutz- und Datensicherungskontrolle

Nach § 33 Abs. 2 Nr. 2 BDSG entfällt die Benachrichtigungspflicht auch dann, wenn die Daten aufgrund gesetzlicher, satzungsgemäßer oder vertraglicher Aufbewahrungsfristen nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen. Die erste Ausnahme des Abs. 2 Nr. 2 ist hinsichtlich der Benachrichtigungspflicht weitgehend gegenstandslos, da die noch aufzubewahrenden Daten

12) Vgl. mit ausführlicher Begründung: Gola/Schomerus (Fn. 9), § 33 Anm. 2.3; anderer Auffassung: Dörr/Schmidt, Neues Bundesdatenschutzgesetz – Handkommentar, 2. Aufl., Köln 1992, § 33 Rn. 8; Schaffland/Wiltfang, Bundesdatenschutzgesetz, Loseblatt, § 33 Rn. 7

13) Gola/Schomerus (Fn. 9), § 33 Anm. 2.3.

14) Vgl. Gola/Schomerus (Fn. 9), § 33 Anm. 2.2; Dörr/Schmidt (Fn. 12), § 33 Rn. 9; Bergmann/Möhrle/Herb, Datenschutzrecht, Loseblattsammlung, § 33 Rn. 43; Simitis/Dammann/Geiger/Mallmann/Walz (Fn. 9), § 33 Rn. 36; sehr weitgehend: Schaffland/Wiltfang (Fn. 12), § 33 Rn. 22, die sogar eine quartalsweise Benachrichtigung für zulässig halten.

15) Vgl. Dörr/Schmidt (Fn. 12), § 33 Rn. 16.

16) Vgl. Bergmann/Möhrle/Herb (Fn. 14), § 33 Rn. 34.

17) Vgl. Bergmann/Möhrle/Herb (Fn. 14), § 33 Rn. 76.

18) Vgl. so z. B Wächter, M., Die Entbehrlichkeit der Benachrichtigung nach § 33 Abs. 2 Nr. 1 BDSG, Computer und Recht 1992, S. 558 ff.

19) Vgl. Dörr/Schmidt (Fn. 12), § 33 Rn. 19.

20) Vgl. Däubler (Fn. 9), S. 477; Dörr/Schmidt (Fn. 12), § 33 Rn. 9.

21) Vgl. Bergmann/Möhrle/Herb (Fn. 14), § 33 Rn. 90 f.

22) Vgl. Gola/Schomerus (Fn. 9), § 33 Anm. 6.2.

zuvor regelmäßig für einen bestimmten Zweck gespeichert wurden, so dass zuvor eine Benachrichtigungspflicht bestanden hat[23]. Dass die ausschließlich der Datensicherung und der Datenschutzkontrolle dienenden Daten nicht der Benachrichtigungspflicht unterliegen, ist hinnehmbar, da § 31 BDSG ein generelles Verbot der Zweckentfremdung dieser Daten enthält[24].

Geheimhaltungspflicht

Nach § 33 Abs. 2 Nr. 3 BDSG entfällt die Benachrichtigung auch dann, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen. In Bezug auf Beschäftigtendaten werden diese Voraussetzungen in der Regel nicht zum Tragen kommen[25].

Gesetzliche Vorschrift

Eine Benachrichtigung entfällt nach § 33 Abs. 2 Nr. 4 BDSG, wenn die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist.

Wissenschaftliche Forschung

Eine Benachrichtigung entfällt nach § 33 Abs. 2 Nr. 5 BDSG, wenn die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde.

Gefährdung der öffentlichen Sicherheit

Nach § 33 Abs. 2 Nr. 6 BDSG entfällt eine Benachrichtigungspflicht, wenn die zuständige öffentliche Stelle gegenüber der speichernden Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde. Diese Regelung kann in Unternehmen von Bedeutung sein, die mit Behörden Vertragsbeziehungen unterhalten, die sich auf geheimhaltungspflichtige Angelegenheiten beziehen[26]. So kann es sich unter Umständen als notwendig erweisen, dass personenbezogene Daten auch gegenüber dem Betroffenen geheimgehalten werden müssen, wenn ein Mitarbeiter unter dem Verdacht geheimdienstlicher Tätigkeit steht[27]. Nach Lage der Dinge kommt eine solche Maßnahme allenfalls im Rahmen der Strafverfolgung in Betracht[28].

Allgemein zugängliche Quellen

Nach § 33 Abs. 2 Nr. 7a BDSG kann die Benachrichtigung dann entfallen, wenn die Daten für eigene Zwecke gespeichert und aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist. Zu den allgemein zugänglichen Quellen zählen insbesondere Printmedien (z. B. Zeitungen, Adressbücher, Branchenverzeichnisse, Telefonbücher) sowie Hörfunk, Fernsehen, Filme und Videos. Darüber hinaus zählen zu den öffentlich zugänglichen Quellen öffentliche Register, wie das Schuldnerverzeichnis (§ 915 ZPO), Handelsregister (§ 9 HGB) etc.[29]. Diese Regelung ist in dieser Form jedoch nicht akzeptabel. Zwar steht nach Art. 5 Abs. 1 Satz 1 GG jedem das Recht zu, sich aus allgemein zugänglichen Quellen zu informieren, jedoch enthält dieses nicht die generelle Befugnis, die Informationen zu speichern oder mit anderen personenbezogenen Daten zu verknüpfen[30].

Gefährdung der Geschäftszwecke

Nach § 33 Abs. 2 Nr. 7b BDSG kann eine Benachrichtigung schließlich entfallen, wenn die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde. Eine Ausnahme soll dann gelten, wenn das Interesse an der Benachrichtigung die Gefährdung überwiegt. In Bezug auf das Arbeitsverhältnis kommen hier nur Betriebs- oder Geschäftsgeheimnisse in Betracht. Dabei wird eine Beeinträchtigung allein nicht genügen, vielmehr muss die Mitteilung dazu führen, dass bestimmte Geschäfte, bspw. aus Kostengründen, unmöglich werden.[31] Betrachtet man jedoch diese Ausnahmen, kommt ihnen im Arbeitsrecht bei sachgerechter Betrachtung keine große Bedeutung zu.[32]

Schriftliche Dokumentation von Ausnahmen und Verstoß gegen die Benachrichtigung

Beruft sich die verantwortliche Stelle auf eine der in § 33 Abs. 2 BDSG aufgeführten Ausnahmen, so hat sie darzulegen, dass sie die Voraussetzungen und deren Vorhandensein sorgfältig geprüft hat[33]. Zudem legt sie **schriftlich** fest, unter welchen der vom Gesetz vorgegebenen Voraussetzungen von einer Benachrichtigung abgesehen wird.

Ein Verstoß gegen die Benachrichtigungspflicht ist gemäß § 43 Abs. 3 BDSG bußgeldbewehrt. Wer den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt, begeht eine Ordnungswidrigkeit[34] (§ 43 Abs. 1 Nr. 8 BDSG).

8. Recht auf Auskunft gemäß § 34 BDSG

Gemäß § 34 Abs. 1 BDSG kann der Betroffene Auskunft verlangen über

- die zu seiner Person gespeicherten Daten,
- die Herkunft,
- den oder die Empfänger oder Kategorien von Empfängern und
- den Zweck der Speicherung.

Das Auskunftsrecht ermöglicht dem Betroffenen den Anspruch auf Mitteilung der **„zu seiner Person gespeicherten Daten"**. Der Begriff ist weiterzufassen als der in § 3 Abs. 1 BDSG verwendete Begriff „personenbezogene Daten", denn er umfasst über jede Einzelangabe, über „persönliche und sachliche Verhältnisse" hinaus, auch Angaben über die gespeicherten Daten. So gehört zu den zur Person gespeicherten Daten auch die Bezeichnung der jeweiligen Dateien[35]. Auch gesperrte Daten unterliegen der Auskunftspflicht.

Zudem muss dem Betroffenen **„Herkunft und Empfänger"** seiner Daten mitgeteilt werden. **„Herkunft"** meint die Quelle, d. h. die Person oder Institution, von der die Information stammt.[36]. Gemeint sind externe Personen und Stellen, wobei auch die Adresse desjenigen, von

23) Vgl. Gola/Schomerus (Fn. 9), § 33 Anm. 6.2.

24) Vgl. Däubler (Fn. 9), S. 477; vgl. auch Bergmann/Möhrle/Herb (Fn. 14), § 33 Rn. 110.

25) Vgl. Däubler (Fn. 9), S. 477.

26) Vgl. Bergmann/Möhrle/Herb (Fn. 14), § 33 Rn. 119.

27) Vgl. Gola/Schomerus (Fn. 9), § 33 Anm. 6.5.

28) Vgl. Däubler (Fn. 9), S. 477.

29) Vgl. Bergmann/Möhrle/Herb (Fn. 14), § 33 Rn. 127 mit weiteren Nachweisen.

30) Vgl. Däubler (Fn. 9), S. 477.

31) Vgl. Gola/Schomerus (Fn. 9), § 33 Anm. 6.8.

32) Vgl. Däubler (Fn. 9), S. 477.

33) Vgl. Gola/Schomerus (Fn. 9), § 44 Rn. 2.3.

34) Vgl. Bergmann/Möhrle/Herb (Fn. 14), § 33 Rn. 151.

35) Vgl. Bergmann/Möhrle/Herb (Fn. 14), § 34 Rn. 38; Hess. VGH, Beschluss vom 17. 12. 1990, Recht der Datenverarbeitung 1991, S. 188.

36) Vgl. Däubler (Fn. 9), S. 478.

dem die Daten stammen, anzugeben ist[37]. **„Empfänger"** sind alle Personen und Institutionen, an die in der Vergangenheit, d.h. bis zur Auskunftserteilung, Daten übermittelt wurden. Dabei ist es gleichgültig, ob es sich um regelmäßige oder einmalige Datenübermittlung gehandelt hat[38]. Der Beschäftigte hat seinerseits dann die Möglichkeit, unzulässigen oder unrichtigen Angaben bis hin zu weiteren Empfängern nachzugehen. Durch diese Regelungen werden die Rechte auf Datenkorrektur über die verantwortliche Stelle hinaus bis in die gesamte Übermittlungskette erleichtert.

Ferner ist dem Betroffenen der **„Zweck der Speicherung"** der Daten mitzuteilen. Hierzu gehört nicht nur der allgemeine Verwendungszusammenhang wie z.B. Produktionssteuerung oder Lohn- und Gehaltsabrechnung, sondern auch die Angabe der eingesetzten Anwendungsprogramme [39].

Das Auskunftsverlangen ist an keine bestimmte Form gebunden und kann somit mündlich, telefonisch oder schriftlich erfolgen. Dabei kann der Betroffene sein Auskunftsverlangen jederzeit an den Arbeitgeber richten und muss dies zudem nicht näher begründen. Er ist jedoch nach § 34 Abs. 1 BDSG verpflichtet, die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher zu bezeichnen. Die Auskunft ist vom Arbeitgeber in schriftlicher Form zu erteilen, wobei die Daten in entschlüsselter Form mitzuteilen sind. Nach § 34 Abs. 5 BDSG ist die Auskunft unentgeltlich.

Auch mit der Novellierung des BDSG kann zwar ein Verstoß gegen die Benachrichtigungspflicht als Ordnungswidrigkeit in § 43 BDSG geahndet werden, unverständlicherweise gilt dieses jedoch nicht bei einem Verstoß gegen das Auskunftsrecht.

Nach § 34 Abs. 4 BDSG gelten die in § 33 Abs. 2 Nr. 2, 3 und 5 bis 7 BDSG für die Benachrichtigungspflicht aufgestellten Ausnahmen auch in bezug auf eine Auskunftserteilung gemäß § 34 BDSG. Diesen Ausnahmen kommt im Arbeitsrecht keine große Bedeutung zu.

9. Recht auf Datenkorrektur und Widerspruch

In § 35 BDSG werden die Rechte der Betroffenen auf Datenkorrektur bei unrichtiger oder unzulässiger Datenverarbeitung geregelt. Es sind dies die Rechte auf

- Berichtigung (§ 35 Abs. 1 BDSG),
- Löschung (§ 35 Abs. 2 BDSG)
- Sperrung (§ 35 Abs. 3 und 4 BDSG)
- Widerspruch (§ 35 Abs. 5 BDSG).

8.1 Anspruch auf Berichtigung

Nach § 35 Abs. 1 BDSG sind personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Die Berichtigung hat unverzüglich zu erfolgen und ist nicht davon abhängig, ob der Betroffene sein Recht geltend macht. Vielmehr ist die verantwortliche Stelle von sich aus verpflichtet, unrichtige Daten zu berichtigen. Die Berichtigungspflicht besteht für unrichtige Daten, also solche Daten, die mit der Realität nicht übereinstimmen. Unrichtigkeit liegt jedoch nicht nur bei offenkundigen Fehlern, unrichtigen Adressen oder unrichtigem Geburtsdatum, sondern auch bei einem so genannten Kontextverlust der Daten vor, der so gravierend ist, dass Fehlinterpretationen zumindest wahrscheinlich sind[40]. Wird bspw. bei einem Beschäftigten nur die Summe der Fehlzeiten gespeichert, ohne dass nach den Gründen wie Krankheit, Urlaub, Weiterbildung etc. differenziert wird, führt dies zu falschen Vorstellungen über die Leistungsfähigkeit eines Arbeitnehmers[41]. Dieses gilt ebenfalls für Werturteile, die auf falschen Tatsachen oder unangemessenen Würdigungen der Tatsachen beruhen, wobei jedoch grundsätzlich anzustreben ist, dass die Speicherung von Werturteilen generell unterbleibt[42].

Eine Berichtigung kann erfolgen, indem

- ein falsches durch ein richtiges Datum ersetzt,
- ein Datum vervollständigt oder
- ein Datum ersatzlos gestrichen wird.

Wurden Daten regelmäßig an Dritte weitergegeben, hat die verantwortliche Stelle diese gemäß § 35 Abs. 7 BDSG von der Berichtigung zu verständigen. Dieses soll jedoch nur gelten, wenn dies keine unverhältnismäßigen Aufwand für die verantwortliche Stelle bedeutet und gleichzeitig schutzwürdige Interessen des Betroffenen dem nicht entgegenstehen.

Das Gesetz schreibt keine bestimmte Frist vor, innerhalb derer die Berichtigung zu erfolgen hat. In jedem Fall wird die Berichtigung so rechtzeitig erfolgen müssen, dass eine weitere Verarbeitung oder Nutzung der unrichtigen Daten nicht mehr stattfindet[43].

9.2 Berichtigung und Löschung von Daten

Nach § 35 Abs. 2 BDSG kann der Betroffene über sein Recht auf Berichtigung hinaus die Löschung seiner Daten verlangen, wenn

- die Speicherung unzulässig war,
- die Richtigkeit besonderer Arten personenbezogener (sensitiver) Daten[44] nicht bewiesen werden kann oder
- die Speicherung der Daten nicht mehr erforderlich ist.

Eine **unzulässige Speicherung** liegt immer dann vor, wenn die Zulässigkeitsvoraussetzungen gemäß § 4 i.V.m. § 28 BDSG nicht gegeben sind. Insbesondere ist zu beachten, dass das BDSG die Datenerhebung mit einbezieht. Nicht rechtmäßig sind Daten dann erhoben worden, wenn das Fragerecht des Arbeitgebers überschritten wurde[45]. Darüber hinaus ist die Speicherung auch dann unzulässig, wenn im Rahmen der Arbeitnehmerbefragung ein Personalfragebogen eingesetzt und der Interessenvertretung das Mitbestimmungsrecht gemäß § 75 Abs. 3 Nr. 8 BPersVG verweigert wurde. Dieses gilt in gleicher Weise für das Mitbestimmungsrecht nach § 75 Abs. 3 Nr. 17 BPersVG in Bezug auf Einführung und Anwendung von technischen Einrichtungen, die dazu geeignet sind, Verhalten oder Leistung der Beschäftigten zu überwachen.

Besonders **sensitive Daten**, nämlich über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Ge-

37) Vgl. Bergmann/Möhrle/Herb (Fn. 14), § 34 Rn. 40.

38) Vgl. Bergmann/Möhrle/Herb (Fn. 23), § 34 Rn. 41.

39) Vgl. Däubler (Fn. 9), S. 478 mit weiteren Nachweisen.

40) Vgl. Däubler (Fn. 9), S. 480; Gola/Schomerus (Fn. 9), § 35 Anm. 2.1.

41) Vgl. Bergmann/Möhrle/Herb (Fn. 14), § 35 Rn. 30; Däubler (Fn. 9), S. 480.

42) Vgl. Gola/Schomerus (Fn. 9), § 35 Anm. 2.1.

43) Vgl. Gola/Schomerus (Fn. 9), § 35 Anm. 2.1.

44) Besondere Arten personenbezogener Daten (sensitive Daten) sind gemäß § 3 Abs. 9 BDSG: „Besondere Arten personenbezogener Daten sind Angaben über die rassische udn ethnische Herkunft, politische Meinungen, religöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben."

45) Vgl. zum Arbeitgeberfragerecht ausführlich: Schierbaum, Erhebung von Bewerber- und Beschäftigtendaten, PersR 1996, S. 261 ff.

werkschaftszugehörigkeit, der Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten, sind zu löschen, wenn ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann. In vielen Fällen wird die Speicherung entsprechender Daten von vornherein unzulässig sein, da der Arbeitgeber nur in Ausnahmefällen danach fragen darf. Soweit der Arbeitgeber ausnahmsweise diese Daten speichern durfte, reicht es für einen Löschungsanspruch aus, wenn der Betroffene die Richtigkeit der gespeicherten Angaben bestreitet. Der Gesetzgeber hat mit dieser Regelung dem besonders sensiblen Charakter dieser Daten Rechnung getragen[46].

Eine Löschung kann zudem verlangt werden, wenn die Kenntnis der Daten für die Erfüllung des Zweckes der **Speicherung nicht mehr erforderlich ist**. Dieses kann sich sowohl auf Daten von erfolglos gebliebenen Bewerbern als auch um Daten von Beschäftigten bzw. ausgeschiedenen Arbeitnehmern beziehen.

9.3 Sperrung von Daten nach § 35 Abs. 3 und Abs. 4 BDSG

In Bezug auf den Löschungsanspruch sieht das BDSG Ausnahmen vor. In § 35 Abs. 3 BDSG werden drei Alternativen aufgestellt, bei denen die Daten nicht gelöscht, sondern in gesperrter Form weitergeführt werden dürfen bzw. müssen. So tritt an Stelle einer Löschung eine Sperrung, wenn

- einer Löschung gesetzliche, satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen (§ 35 Abs. 3 Nr. 1 BDSG),
- Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden (§ 35 Abs. 3 Nr. 2 BDSG) oder
- eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit verhältnismäßig hohem Aufwand möglich ist (§ 35 Abs. 3 Nr. 3 BDSG).

Zudem ist eine Sperrung nach § 35 Abs. 4 BDSG vorgesehen, wenn die Richtigkeit der gespeicherten Daten vom Betroffenen und der speichernden Stelle unterschiedlich beurteilt wird und keine Klärung erreichbar ist. In § 35 Abs. 7 BDSG sind die Folgen für die verantwortliche Stelle aufgeführt, die mit der Sperrung von Daten verbunden sind. So ist die Übermittlung und Nutzung gesperrter Daten nur zulässig, wenn es zu wissenschaftlichen Zwecken unerlässlich, zur Behebung einer bestehenden Beweisnot oder aus sonstigen, im Interesse der speichernden Stelle oder eines Dritten liegenden Gründe unerlässlich ist. Voraussetzung hierfür ist, dass die Daten überhaupt genutzt und übermittelt werden dürften, wenn sie nicht gesperrt wären.

9.4 Recht auf Widerspruch

Die Benachrichtigungs- und Auskunftsrechte werden um ein Widerspruchsrecht ergänzt (§ 35 Abs. 5 BDSG). Es wird Art. 14 EG-Datenschutzrichtlinie umgesetzt, so dass der Betroffene in den Datenverarbeitungsprozess dahingehend eingreifen kann, die Verarbeitung – auch im Falle ihrer Rechtmäßigkeit – zu untersagen. Das Widerspruchsrecht greift ein, soweit der Betroffene der Datenverarbeitung bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation dem Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Das Widerspruchsrecht gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten verpflichtet. Da im Arbeitsleben Datenverarbeitung immer nur sehr eng an der Zweckbestimmung des Arbeitsvertragsverhältnisses erfolgen darf, wird dieses Widerspruchsrecht nur selten zum Tragen kommen kann. Denkbar ist das Widerspruchsrecht, wenn die Rechtmäßigkeit der Datenverarbeitung durch Einwilligung des Beschäftigten begründet wird.

10. Verpflichtung auf das Datengeheimnis

Nach § 5 BDSG ist es den bei der Datenverarbeitung beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei **nicht-öffentlichen Stellen** (Privatbetriebe, Vereine, Stiftungen) beschäftigt werden, bei Aufnahme der Tätigkeit auf das Datengeheimnis zu verpflichten. Dabei besteht das Datengeheimnis auch nach Beendigung der Tätigkeit fort.

Die Vorschrift des § 5 BDSG beinhaltet ein umfassendes gesetzliches Verbot unbefugter Datenverarbeitung. Die Verwendung des Begriffes „unbefugt" hat nur deklaratorische Bedeutung. Dadurch soll hervorgehoben werden, dass befugte Datenverarbeitung nur diejenige ist, die sich nach den Bestimmungen des BDSG vollzieht. Eine Erhebung, Verarbeitung oder Nutzung ist immer dann unbefugt, wenn sie rechtswidrig geschieht. Darunter sind alle Möglichkeiten der unzulässigen Verwendung von Daten zu verstehen, wie z. B.[47]:

- Auswertungen für eigene/private Zwecke;
- Bekanntgabe von Daten an Dritte ohne Rechtsgrundlage (etwa zum Zweck der Wirtschaftspionage);
- Herausgabe von Datenträgern an unbefugte Dritte;
- Entwendung von Datenträgern (etwa zum Zweck der Veräußerung sowie Verkauf von Kundendateien);
- einem Dritten Gelegenheit zu geben, damit dieser Daten abrufen oder Datenträger entwenden kann;
- unzulässiger Abruf von Daten.

Von einer Verpflichtung betroffen sind die „bei der Datenverarbeitung beschäftigten Personen". In erster Linie sind dieses die im DV-Bereich eingesetzten Mitarbeiter, aber auch diejenigen, die in den Fachabteilungen personenbezogene Daten verarbeiten. Die Verpflichtung selbst ist an keine besonderen Formvorschriften gebunden. Insbesondere eine zustimmende Erklärung dessen, der verpflichtet wird, ist nicht erforderlich Es reicht allerdings nicht aus, die Verpflichtungserklärung durch Anhang an das schwarze Brett bekannt zu machen. Erforderlich ist vielmehr die Verpflichtung in jedem Einzelfall[48]. Aus Beweissicherungsgründen sollte die Verpflichtung durch die Unterschrift des Betroffenen bestätigt werden. Die Verpflichtung erfüllt nur dann ihren vom Gesetz beabsichtigten Zweck, wenn sie mit einer Unterweisung des Beschäftigten über seinen besonderen Verpflichtungen nach dem BDSG verbunden sind[49]. Die Mitteilung des Wortlautes des § 5 BDSG reicht nicht aus.

46) Vgl. Däubler (Fn. 9), S. 481.

47) Die Beispiele sind entnommen aus: Bergmann/Möhrle/Herb (Fn. 14), § 5 Rn. 4.

48) Vgl. Gola/Schomerus (Fn. 9), § 5 Anm. 3.1; anderer Auffassung: Schaffland/Wiltfang (Fn. 12), § 5 Rn. 18.

49) Vgl. Gola/Schomerus (Fn. 9), § 5 Anm. 3.3; Auernhammer, Bundesdatenschutzgesetz, 2. Aufl., § 5 Rn. 9.

Der Beschäftigte kann sich bei einem Verstoß gegen das Datengeheimnis nach § 43 BDSG strafbar machen und sich auch Schadensersatzansprüchen aussetzen. Darüber hinaus können arbeitsvertragliche Sanktionen, wie Abmahnung oder Kündigung in Betracht kommen[50]. Eine Kündigung des Arbeitsverhältnisses scheidet jedenfalls dann aus, wenn die fragliche Verletzung des Datengeheimnisses überwiegend durch den Arbeitgeber z. B. aufgrund fehlerhafter Organisation verursacht wurde.

11. Schadensersatz

Die §§ 7 und 8 BDSG enthalten eine **eigenständige Anspruchsgrundlage** für den Betroffenen (Beschäftigten), um gegenüber nicht-öffentlichen und öffentliche Stellen **Schadensersatz** geltend zu machen. Schadensersatzansprüche können geltend gemacht werden, wenn eine verantwortliche Stelle einem Betroffenen eine nach dem BDSG oder anderer Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zufügt (§ 7 BDSG). Dabei muss der Betroffene der datenverarbeitende Stelle nicht ein **Verschulden nachweisen.** Denn in Anbetracht der komplexen, für außenstehende Dritte kaum nachvollziehbaren Vorgängen bei der automatisierten Verarbeitung kann es dem Betroffenen nicht zugemutet werden, dem Betreiber der Datenverarbeitung ein Verschulden nachzuweisen.

Der für die Verarbeitung Verantwortliche kann von der Haftung befreit werden, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zur Last gelegt werden kann. Im Gesetz heißt es: „Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat." (§ 7 Satz 2 BDSG) § 8 BDSG enthält entsprechende Vorgaben wie der § 7 BDSG richtet sich aber ausschließlich an öffentliche Stellen. Festgelegt wird u. a., dass bei einer schweren Verletzung des Persönlichkeitsrechts dem Betroffene, der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen ist, wobei hier zusätzlich u. a. die Höhe der Schadenersatzansprüche auf 250 000,– DM begrenzt.

Bruno Schierbaum,
BTQ Niedersachsen, Oldenburg

50) Vgl. Däubler/Klebe/Wedde, Bundesdatenschutzgesetz, § 5 Rn. 16.