Datenverarbeitung in Dienst- und Arbeitsverhältnissen

Rechte der Beschäftigten auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung

Mit dem Einzug von EDV-Systemen in Behörden und Verwaltungen werden auch zunehmend personenbezogene Daten der Beschäftigten verarbeitet. Es kommen z. B. Personalabrechnungssysteme, Zeiterfassungssysteme, Personal- und Stellenverwaltungssysteme, Bürokommunikationssysteme und Telefonnebenstellenanlagen zum Einsatz. Durch diese Entwicklung gewinnt der Datenschutz im Sinne von Schutz der Persönlichkeitsrechte der Betroffenen und damit die Umsetzung des Bundesdatenschutzgesetzes (BDSG) bzw. der einschlägigen Landesdatenschutzgesetze an Bedeutung.

Nach der Rechtssprechung des Bundesverfassungsgerichtes[1]) bildet das Recht auf informationelle Selbstbestimmung, das auch die Datentransparenz umfaßt, eine wesentliche Voraussetzung für die Umsetzung des Datenschutzes. Der einzelne muß wissen, wo welche Daten über ihn gespeichert werden. Hierzu räumen das BDSG bzw. die Landesdatenschutzgesetze den Beschäftigten die Rechte auf Benachrichtigung[2]), Auskunft, Berichtigung, Löschung und Sperrung ein. Da diese Rechte auch als Kernstück des Datenschutzes gesehen werden[3]), aber davon in der Praxis wenig Gebrauch gemacht wird[4]), scheint es angezeigt, auf die entsprechenden rechtlichen Regelungen näher einzugehen.

1. Beschäftigte im öffentlichen Dienst und Datenschutz

Sollen personenbezogene Daten der Beschäftigten erhoben, verarbeitet und genutzt werden, wird in der Regel die Zulässigkeit der Datenverarbeitung aus den Datenschutzgesetzen herzuleiten sein. Aufgrund der unterschiedlichen gesetzlichen Regelungen, dem BDSG[5]), den daneben geltenden Landesdatenschutzgesetzen[6]) und anderen Rechtsvorschriften zum Datenschutz herrscht insbesondere für die Beschäftigten im öffentlichen Dienst eine gewisse Unübersichtlichkeit und somit auch Unklarheit, welche gesetzlichen Regelungen anzuwenden sind. Das BDSG nennt in § 1 Abs. 2 BDSG für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten drei Adressaten:

- Öffentliche Stellen des Bundes,
- Öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesdatenschutzgesetze geregelt ist und
- nicht-öffentliche Stellen (Privatbetriebe).

Für die öffentlichen Stellen des Bundes findet insbesondere der zweite Abschnitt des BDSG, §§ 12–26 BDSG, Anwendung. Für öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Stellen am Wettbewerb teilnehmen, gilt gemäß § 27 BDSG insbesondere der dritte Abschnitt des BDSG, der für die Privatbetriebe gilt[7]). Da mittlerweile alle Bundesländer Datenschutzgesetze erlassen haben, ist für die öffentlichen Stellen der Länder und Gemeinden das Datenschutzgesetz des jeweiligen Bundeslandes anzuwenden. Für nicht-öffentliche Stellen (Privatbetriebe) gilt insbesondere der dritte Abschnitt des BDSG.

Allein vor diesem Hintergrund wird deutlich, daß im Interesse der Beschäftigten ein eigenständiges Arbeitnehmerdatenschutzgesetz lange überfällig ist. Zwar hält die Bundesregierung es für geboten, daß der Schutz der Arbeitnehmerdaten gesetzlich geregelt wird, jedoch ist es bis heute nicht gelungen, einen entsprechenden Entwurf für ein Arbeitnehmerdatenschutzgesetz vorzulegen[8]).

Damit Beschäftigte im öffentlichen Bereich und in der Privatwirtschaft unter datenschutzrechtlichen Aspekten gleichbehandelt werden, verweist das BDSG in bezug auf den Arbeitnehmerdatenschutz im öffentlichen Bereich in § 12 Abs. 4 auf den für Privatbetriebe geltenden dritten Abschnitt des BDSG. Nach § 12 Abs. 4 BDSG sind auf die Verarbeitung von Daten für frühere, bestehende oder künftige dienst- und arbeitsrechtliche Rechtsverhältnisse durch öffentliche Stellen des Bundes die Bestimmungen des dritten Abschnittes über die Datenspeicherung, -übermittlung und -nutzung, § 28 Abs. 1 und 2 Nr. 1 sowie die §§ 33–35 BDSG, anzuwenden. Für die Beschäftigten bei öffentlichen Stellen der Länder und Gemeinden ist die Rechtslage uneinheitlich. Einige Datenschutzgesetze der Länder, wie die Datenschutzgesetze Baden-Württemberg (§ 2 Abs. 2 BaWü) und Rheinland-Pfalz (§ 2 Abs. 2 RhPf), verweisen wie § 12 Abs. 4 BDSG für öffentliche Stellen des Bundes ebenfalls

---

1) Vgl. BVerfG, Urteil v. 15. 12. 1983, NJW 8/84, S. 419 ff.

2) Eine Benachrichtigung der Beschäftigten ist in einigen Landesdatenschutzgesetzen nicht vorgesehen, was u. a. damit begründet wird, daß das Prinzip der Direkterhebung beim Betroffenen eine Benachrichtigung erübrigt. Siehe Abb. 2.

3) Vgl. Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, München 1992, S. 132.

4) Es wird davon ausgegangen, daß in der Privatwirtschaft lediglich 2 bis 3 % der Arbeitnehmer von diesen Rechten Gebrauch machen. Vgl. Wohlgemuth, Datenschutz für Arbeitnehmer, 2. Aufl., Neuwied 1988, S. 176 mit weiteren Nachweisen. Es muß davon ausgegangen werden, daß dieses im öffentlichen Bereich nicht anders aussieht. In diesem Zusammenhang wird zu Recht auf die komplizierte und wenig anwenderfreundliche Gesetzgebungstechnik hingewiesen. Vgl. Bergmann/Möhrle/Herb, Datenschutzrecht, Loseblattsammlung, Stand 1/93, § 33 Rn. 22.

5) Das BDSG vom 20. 12. 1990 ist im BGBl. I, S. 2955 verkündet worden und am 1. 6. 1991 in Kraft getreten. Es ist als Art. 1 Teil des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. 12. 1990. Das novellierte BDSG löst das Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 27. 1. 1977, das am 1. 1. 1978 in Kraft getreten ist, ab.

6) Vor dem Hintergrund des Volkszählungsurteils sind mittlerweile alle Landesdatenschutzgesetze novelliert worden.

7) Die meisten Landesdatenschutzgesetze enthalten für öffentlichrechtliche Wettbewerbsunternehmen ähnliche Regelungen.

8) Vgl. hierzu Auernhammer, Bundesdatenschutzgesetz, Köln 1993, § 12 Rn. 19 mit weiteren Nachweisen; Gola/Wronka, Handbuch für den Arbeitnehmerdatenschutz, Köln 1989, S. 27 ff.; Stange, Datenschutz, Berlin 1992, S. 173; Lübking, Datenschutz in der Kommunalverwaltung, Berlin 1993, S. 179 ff.

auf den dritten Abschnitt des BDSG. Ansonsten enthalten die Landesdatenschutzgesetzes eigene, teilweise vom BDSG abweichende, Regelungen. Zudem enthalten einige Landesdatenschutzgesetze Sonderregelungen in bezug auf den Datenschutz in Dienst- und Arbeitsverhältnissen.

2. Zulässigkeit der Verarbeitung personenbezogener Daten

Das BDSG hat den Zweck, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG)[9]. Geschütztes Rechtsgut sind demnach nicht die Daten als solche, sondern das individuelle Recht auf Achtung der persönlichen und privaten Sphäre. Der im BDSG und in den Landesdatenschutzgesetzen verwendete Begriff „personenbezogene Daten" ist dabei umfassender als der in diesem Zusammenhang mit der Datenverarbeitung verwendete Begriff „Personaldaten".

Personenbezogene Daten, die von den Datenschutzgesetzen geschützt werden, sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (§ 3 Abs. 1 BDSG). Läßt sich allein auf der Basis der Daten eine Person bestimmen oder ist bspw. mit dem Zusatzwissen eines Sachbearbeiters eine Person bestimmbar, sind dieses von den Datenschutzgesetzen zu schützende personenbezogene Daten. So handelt es sich häufig bei Daten, die auf dem ersten Blick anonym erscheinen oder auch bei Sachdaten, wie Zeiterfassungsdaten oder Telefonverbindungsdaten, um personenbezogene Daten.

Zur Wahrung der Persönlichkeitsrechte der Betroffenen gehen das BDSG und die Landesdatenschutzgesetze in bezug auf Verarbeitung und Nutzung personenbezogener Daten von einem Verbot mit Erlaubnisvorbehalt aus. D. h. die Verarbeitung und Nutzung personenbezogener Daten ist gemäß § 4 Abs. 1 BDSG grundsätzlich verboten und nur dann erlaubt bzw. zulässig, wenn

- der Betroffene eingewilligt hat.
- eine spezielle Rechtsvorschrift dieses erlaubt oder
- das BDSG selbst dieses erlaubt.

Die speichernde Stelle hat für jedes personenbezogene Datum von sich aus vor der Verarbeitung und Nutzung die Zulässigkeitsvoraussetzungen zu prüfen. Hierzu bedarf es also grundsätzlich nicht der Veranlassung durch den Betroffenen oder durch den Personalrat.

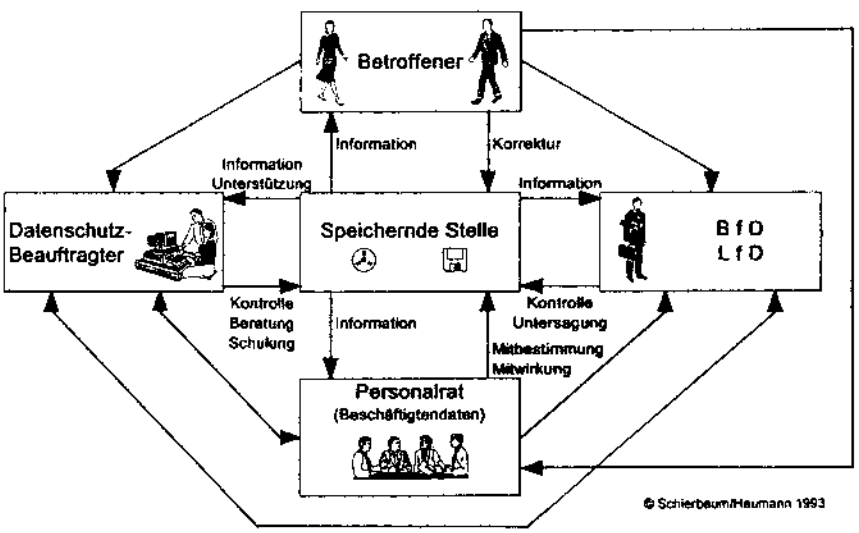
3. Kontrollinstanzen des Datenschutzes

Im Rahmen der Sicherstellung des Datenschutzes kommt einer wirksamen Kontrolle ein hoher Stellenwert zu. In der Abbildung „Das Kontrollsystem im öffentlichen Dienst" sind die Kontrollinstanzen dargestellt, die jeweils einen unterschiedlichen Beitrag zu einer Kontrolle leisten können.

So sehen die Landesdatenschutzgesetze Berlins (§ 18 Abs. 4 BlnDSG), Hessens (§ 5 Abs. 2 HDSG) und Niedersachsens (§ 8 Abs. 3 NDSG) die Bestellung eines internen behördlichen Datenschutzbeauftragten vor. Diese haben u. a. die Aufgabe, die Einhaltung der einschlägigen Datenschutzvorschriften sicherzustellen. Wo eine Bestellung eines internen Datenschutzbeauftragten nicht gesetzlich vorgeschrieben ist, kann es sich jedoch für die Behörde als notwendig erweisen, einen Datenschutzbeauftragten zu bestellen[10], um die Datenschutzgesetze umzusetzen.

Als externe Kontrollinstanzen kommt dem Bundesbeauftragten für den Datenschutz (BfD) und den Landesdatenschutzbeauftragten (LfD) die Aufgabe zu, die Einhaltung der jeweiligen Datenschutzgesetze und anderer Vorschriften zum Datenschutz zu kontrollieren[11]. Der Personalrat hat gemäß § 68 Abs. 1 Nr. 2 Bundespersonalvertretungsgesetz (BPersVG) darüber zu wachen, daß die zugunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge und Verwaltungsordnungen durchgeführt werden. Beim BDSG handelt es sich um ein Gesetz im Sinne des § 68 Abs. 1 Nr. 2 BPersVG. In den Personalvertretungsgesetzen der Länder finden sich entsprechende Regelungen[12]. Der einzelne Beschäftigte seinerseits kann durch die Wahrnehmung seiner Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung eine gewisse Kontrollfunktion ausüben. Zudem trägt die Wahrnehmung dieser

Das Kontrollsystem im öffentlichen Bereich



9) In den Landesdatenschutzgesetzen finden sich ähnliche Formulierungen zum Zweck der Gesetze, wobei in einigen Datenschutzgesetzen vor dem Hintergrund des Volkszählungsurteils das „Recht auf informationelle Selbstbestimmung" herausgestellt wird. So lautet z. B. § 1 NDSG folgendermaßen: „Aufgabe dieses Gesetzes ist es, 1. das Recht einer jeden Person zu gewährleisten, selbst die Preisgabe und Verwendung ihrer Daten zu bestimmen (Recht auf informationelle Selbstbestimmung), 2. einer Beeinträchtigung der Wirkungsmöglichkeiten der Verfassungsorgane des Landes und der Organe der kommunalen Gebietskörperschaften infolge der automatisierten Datenverarbeitung entgegenzuwirken. Dieses Gesetz bestimmt, unter welchen Voraussetzungen personenbezogene Daten durch öffentliche Stellen verarbeitet werden dürfen."

10) Vgl. Auernhammer, (Fn. 8), § 18 Rn. 2 und Rn. 18; Gola/Wronka (Fn. 8), S. 253 f. jeweils mit weiteren Nachweisen; vgl. auch Stange (Fn. 8), S. 131; Lübking (Fn. 8), S. 233 ff.

11) Vgl. ausführlich Stange (Fn. 8), S. 151 ff.

12) Vgl. Altvater u. a., Bundespersonalvertretungsgesetz, Köln 1990, § 68 Rn. 3 und Rn. 27.

Rechte zu einer größeren Datentransparenz bei.

4. Datentransparenz

Das Bundesverfassungsgericht hat in seinem Urteil vom 15. 12. 1983[13]) aus Art. 1 Abs. 1 und Art. 2 Abs. 1 Grundgesetz ein Recht eines jeden auf **informationelle Selbstbestimmung** abgeleitet. In der Erkenntnis der mit der modernen Datenverarbeitung verbundenen Gefahren für die Betroffenen führt das Gericht aus: „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus." Zudem stellt das Gericht das Recht des 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.

Für die Existenz und Ausübung des Rechts auf informationelle Selbstbestimmung bildet Datentransparenz eine wesentliche Voraussetzung[14]). Das Bundesverfassungsgericht führt dazu aus: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner 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 wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen, wer was bei welcher Gelegenheit über sie weiß."[15]) Transparenz der gespeicherten Daten gehört somit zu den verfassungsrechtlich gewährleisteten Grundpositionen der Betroffenen. Im folgenden werden die Rechte der Beschäftigten auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung dargestellt.

5. Rechte der Beschäftigten nach dem BDSG

Das BDSG enthält eine Reihe von Rechtsansprüchen der Betroffenen. Durch den Verweis des § 12 Abs. 4 BDSG gelten die §§ 33–35 BDSG nicht nur für die Beschäftigten in Privatbetrieben (nicht-öffentlicher Bereich), sondern auch für die Beschäftigten im öffentlichen Bereich. Für die Länder sind die entsprechenden Rechte in den Landesdatenschutzgesetzen verankert. Im folgenden soll insbesondere auf die Rechte im BDSG eingegangen werden, wobei die entsprechenden Regelungen der Landesdatenschutzgesetze der gegenüberstehenden Abbildung „Rechte der Beschäftigten nach den Datenschutzgesetzen" zu entnehmen sind. Folgende Rechte werden den Beschäftigten im öffentlichen Dienst nach dem BDSG eingeräumt:

- Benachrichtigung (§ 33 BDSG).
- Auskunft (§ 34 Abs. 1 BDSG).
- Berichtigung (§ 35 Abs. 2 BDSG).
- Löschung (§ 35 Abs. 2 BDSG).
- Sperrung (§ 35 Abs. 4 BDSG).
- Schadensersatz (§ 7 BDSG).

Diese Rechte sind gemäß § 6 Abs. 1 BDSG unabdingbar und können durch ein Rechtsgeschäft weder ausgeschlossen noch beschränkt werden. Demzufolge sind Vereinbarungen oder Absprachen, die diese Rechte ganz oder teilweise einschränken, unwirksam[16]). Dieses gilt sowohl für den Abschluß von Einzelverträgen als auch für den Abschluß von Dienstvereinbarungen. Da das Recht auf informationelle Selbstbestimmung (Datentransparenz) ein bedeutendes Rechtsgut darstellt, ist es nur konsequent, daß durch § 6 BDSG die Vertragsfreiheit eingeschränkt wird[17]). Denn insbesondere in Abhängigkeitsverhältnissen, wie in Arbeitsverhältnissen, ist der schwächere Vertragspartner (der Beschäftigte) eher bereit, auf seine Rechte zu verzichten[18]). Die Landesdatenschutzgesetze enthalten in bezug auf die Unabdingbarkeit der Rechte der Betroffenen entsprechende Regelungen.

5.1 Die Benachrichtigung des Beschäftigten nach § 33 BDSG

Werden erstmals personenbezogene Daten des Beschäftigten gespeichert, ist er gemäß § 33 Abs. 1 BDSG von der **Speicherung** selbst und der **Art der gespeicherten Daten** zu benachrichtigen. In § 33 Abs. 2 BDSG sind eine Reihe von Ausnahmen von der Benachrichtigungspflicht festgelegt worden. Der Benachrichtigung wird jedoch mit der Novellierung des BDSG u. a. dadurch besondere Bedeutung beigemessen, daß ihr im Gegensatz zum „alten" BDSG ein eigener Paragraph eingeräumt wird.

Voraussetzung für eine Benachrichtigung ist, daß der Arbeitgeber erstmals personenbezogene Daten der Beschäftigten speichert. Eine Benachrichtigung hat somit zu erfolgen, wenn über einen einzelnen Daten gespeichert werden, zu dessen Person bisher nichts gespeichert wurde. Werden jedoch im Laufe eines Beschäftigungsverhältnisses zusätzliche neue Daten, z. B. 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[19]). „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 kein Gebrauch machen, während inzwischen durch Änderung der gespeicherten Datenarten sein Persönlichkeitsrecht tangierende Verarbeitungen stattfinden."[20])

Eine Benachrichtigung, die unverzüglich, also ohne schuldhaftes Zögern (§ 121 Abs. 1 BGB), nach erstmaliger Speicherung zu erfolgen hat, wird dem Betroffenen spätestens 2 Wochen nach der erstmaligen Speicherung „zugehen" müssen[21]).

---

13) Vgl. BVerfG, Urteil v. 15. 12. 1983, NJW 8/84, S. 419 f.

14) Vgl. Däubler, Individualrechte des Arbeitnehmers nach dem neuen BDSG, CR 8/91, S. 476; Ordemann/Schomerus/Gola, Bundesdatenschutzgesetz mit Erläuterungen, München 1992, § 33 Anm. 3.3.

15) BVerfG, Urteil v. 15. 12. 1983, NJW 8/84, S. 419.

16) Vgl. Auernhammer (Fn. 8), § 6 Rn. 8.

17) Vgl. Däubler (Fn. 14), S. 482; vgl. auch Auernhammer (Fn. 8), § 6 Rn. 9.

18) Vgl. Däubler (Fn. 14), S. 482.

19) Vgl. mit ausführlicher Begründung: Ordemann/Schomerus/Gola (Fn. 14), § 33 Anm. 2.2; so wohl auch Bergmann/Möhrle/Herb (Fn. 4), § 33 Rn. 57; anderer Auffassung: Dörr/Schmidt, Neues Bundesdatenschutzgesetz, 2. Aufl., Köln, 1992, § 33 Rn. 8; Schaffland/Wiltfang, Bundesdatenschutzgesetz, Loseblattsammlung, Stand: 3/1993, § 33 Rn. 7.

20) Ordemann/Schomerus/Gola (Fn. 14), § 33 Anm. 2.2.

21) Vgl. Auernhammer (Fn. 8), § 33 Rn. 8 mit weiteren Nachweisen; Ordemann/Schomerus/Gola (Fn. 14), § 33 Anm. 2.2; Wohlgemuth (Fn. 4), S. 109; Bergmann/Möhrle/Herb (Fn. 4), § 33 Rn. 43; sehr weitgehend Schaffland/Wiltfang (Fn. 19), § 33 Rn. 22, die sogar eine quartalsweise Benachrichtigung für zulässig halten.

Rechte der Beschäftigten nach den Datenschutzgesetzen

	Benach-richtigung	Auskunft	Berichtigung	Löschung	Sperrung	Schadensersatz	dienst- und arbeitsrechtl. Verhältnisse
BDSG	§ 33	§ 34	§ 35 Abs. 1	§ 35 Abs. 2	§ 35 Abs. 4	§ 7	—
Baden-Württemberg[1]	§ 33 BDSG[2]	§ 34 BDSG	§ 35 Abs. 1 BDSG	§ 35 Abs. 2 BDSG	§ 35 Abs. 4 BDSG	§ 21 LDSG	—
Bayern[3]	—	Art 10	Art. 11	Art. 12 Abs. 1	Art. 12 Abs. 2–5	Art. 14	—
Berlin[4]	§ 15 Abs. 2	§ 15 Abs. 1	§ 16 Abs. 1	§ 16 Abs. 3	§ 16 Ab s. 2	§ 17	—
Brandenburg[5]	§ 18 Abs. 2	§ 18 Abs. 1	§ 19 Abs. 1	§ 19 Abs. 2	§ 19 Abs. 3	§ 20	§ 29
Bremen[6]	—	§ 19	§ 20 Abs. 1	§ 20 Abs. 3	§ 20 Abs. 2	—	§ 22
Hamburg[7]	—	§ 18	§ 19 Abs. 1	§ 19 Abs. 3	§ 19 Abs. 2	§ 20	§ 28
Hessen[8]	§ 18 Abs. 2	§ 18 Abs. 1	§ 19 Abs. 1	§ 19 Abs. 3 u. 4	§ 19 Abs. 2	§ 20	§ 34
Mecklenburg-Vorpommern[9]	—	§ 20	§ 11 Abs. 1	§ 11 Abs. 2	§ 21	§ 23	§ 31
Nieder-sachsen[10]	§ 24 Abs. 1	k§ 16	§ 17 Abs. 1	§ 17 Abs. 2	§ 17 Abs. 3	§ 18	§ 24
Nordrhein-Westfalen[11]	—	§ 18	§ 19 Abs. 1	§ 19 Abs. 3	§ 19 Abs. 2	§ 20	§ 29
Rheinland-Pfalz[12]	§ 33 BDSG[13]	§ 34 BDSG	§ 35 Abs. 1 BDSG	§ 35 Abs. 2 BDSG	§ 35 Abs. 4 BDSG	§ 16 LDatG	—
Saarland[14]	—	§ 18	§ 19 Abs. 1	§ 19 Abs. 3	§ 19 Abs. 2	§ 20	§ 29
Sachsen[15]	—	§ 17	k§ 18	§ 19	§ 20	§ 21	§ 31
Sachsen-Anhalt[16]	§ 9 Abs. 3[17]	§ 15	§ 16 Abs. 1	§ 16 Abs. 2	§ 16 Abs. 3 u. 4	§ 18	§ 28
Schleswig-Holstein[18]	—	§ 18	§ 19 Abs. 1	§ 19 Abs. 3	§ 19 Abs. 2	§ 21	§ 30
Thüringen[19]	—	§ 13	§ 14	§ 16	§ 15	§ 18	—

1) Baden-Württemberg
Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz – LDSG) vom 27. 5. 1991, GBl. S. 277.

2) Gemäß § 2 Abs. 2 LDSG-BaWü gelten für die Verarbeitung personenbezogener Daten im Rahmen früherer, bestehender oder zukünftiger dienst- oder arbeitsrechtlicher Rechtsverhältnisse anstelle von § 5 Satz 1 Nr. 1 u. 2 sowie §§ 11 bis 20 LDSG-BaWü der § 28 Abs. 1 u. 2 sowie die §§ 33 bis 35 BDSG.

3) Bayern
Bayerisches Datenschutzgesetz (BayDSG) vom 23. 7. 1993, BayGVBl. Nr. 19/1993, S. 498; gemäß Art. 39 tritt das Gesetz am 1. März 1994 in Kraft.

4) Berlin
Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG) in der Fassung vom 17. 11. 1990, GVBl. 1991, S. 16.

5) Brandenburg
Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BrDSG) vom 20. 1. 1992, GVBl. I, S. 2.

6) Bremen
Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bremisches Datenschutzgesetz – BrDSG) in der Fassung der Bek. vom 14. 10. 1987, Gbl. S. 263.

7) Hamburg
Hamburgisches Datenschutzgesetz (HmbDSG) vom 5. 7. 1990, GVBl. S. 133.

8) Hessen
Hessisches Datenschutzgesetz (HDSG) vom 11. 11. 1986, GVBl. S. 309, geändert durch Ges. vom 21. 12. 1988, GVBl. S. 424.

9) Mecklenburg-Vorpommern
Gesetz zum Schutz des Bürgers beim Umgang mit seinen Daten (Landesdatenschutzgesetz von Mecklenburg-Vorpommern – DSG-MV) vom 24. 7. 1992, GVBl. S. 487.

10) Niedersachsen
Niedersächsisches Datenschutzgesetz (NDSG) vom 17. 7. 1993, GVBl. Nr. 19/1993.

11) Nordrhein-Westfalen
Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen – DSG NW) vom 15. 3. 1988, GVBl. S. 160.

12) Rheinland-Pfalz
Landesgesetz zum Schutze des Bürgers bei der Verarbeitung personenbezogener Daten (Landesdatenschutzgesetz – LDatG) vom 21. 12. 1978, GVBl. S. 749, zuletzt geändert durch Ges. vom 13. 2. 1991, GVBl. S. 46.

13) Gemäß § 2 Abs. 3 LDatG-RP gelten anstelle der §§ 5, 6, 7, 12 und 13 LDatG-RP die §§ 22 und 24 Abs. 1 sowie die §§ 25 bis 27 BDSG vom 27. 1. 1977 in der jeweils geltenden Fassung. Mit der Novellierung des BDSG gelten der § 28 Abs. 1 u. 2 sowie die §§ 33 bis 35 BDSG.

14) Saarland
Saarländisches Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Saarländisches Datenschutzgesetz – SDSG) vom 24. 3. 1993, ABl. des Saarlandes vom 16. 4. 1993, S. 286.

15) Sachsen
Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz – SächsDSG) vom 11. 12. 1991, GVBl. S. 401.

16) Sachsen-Anhalt
Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) vom 12. 3. 1992, GVBl. S. 152.

17) Benachrichtigung bei Erhebung ohne Kenntnis des Betroffenen.

18) Schleswig Holstein
Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz – LDSG) vom 30. 10. 1991, GVBl. S. 555.

19) Thüringen
Thüringer Datenschutzgesetz (ThürDSG) vom 29. 10. 1991, GVBl. S. 516.

Das Gesetz schreibt für die Benachrichtigung keine bestimmte Form vor. Sie liegt im Ermessen der speichernden Stelle und kann mündlich, telefonisch oder schriftlich erfolgen[22]). Allerdings sollte aus Beweissicherungsgründen vor dem Hintergrund der Vergänglichkeit des gesprochenen Wortes die Schriftform gewählt werden. Damit kann sich die speichernde Stelle gegen mögliche Vorwürfe absichern, sie habe die Benachrichtigung unterlassen und damit eine Ordnungswidrigkeit nach § 44 Abs. 1 Nr. 3 BDSG begangen[23]). Dabei wird die Benachrichtigung mit Hilfe einer Postkarte oder eines Telefaxes datenschutzrechtlich bedenklich sein, wenn nicht gewährleistet ist, daß die Information nur den Betroffenen und nicht andere Personen erreicht[24]).

5.2 Wegfall 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 auszulegen[25]); „sie werden in der Praxis seltene Ausnahme bleiben."[26])

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[27]).

Diese Auffassung kann nicht geteilt werden. Die reine Möglichkeit der Kenntniserlangung durch den Betroffenen reicht nicht aus, um der Benachrichtigungspflicht gerecht zu werden, vielmehr muß der Betroffene diese Kenntnis auch tatsächlich erlangt haben[28]). Bestehen für den Beschäftigten keine erkennbaren Anhaltspunkte, muß er nicht mit einer Datenverarbeitung rechnen. Maßstab hierfür kann nicht der auf Feinheiten achtende EDV-Fachmann sein, sondern diejenige Erwartung, die ein Beschäftigter dem Arbeitgeber unter vergleichbaren Arbeitsbedingungen in der Branche üblicherweise entgegenbringt[29]). Etwaige Unsicherheiten dürfen nicht zu Lasten des Betroffenen gehen[30]). D.h. bei Zweifeln über das tatsächliche Wissen des Betroffenen ist die Benachrichtigung vorzunehmen[31]).

Nach **§ 33 Abs. 2 Nr. 2 BDSG** entfällt die Benachrichtigungspflicht auch dann, wenn die Daten aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder Datenschutzkontrolle dienen. Die erste Ausnahme des Abs. 2 Nr. 2 ist hinsichtlich der Benachrichtigungspflicht weitgehend gegenstandslos, da die noch aufzubewahrenden Daten zuvor regelmäßig für einen bestimmten Zweck gespeichert wurden, so daß zuvor eine Benachrichtigungspflicht bestanden hat[32]). Daß die ausschließlich der Datensicherung und des Datenschutzkontrolle dienenden Daten nicht der Benachrichtigungspflicht unterliegen, ist hinnehmbar, da § 31 BDSG ein generelles Verbot der Zweckentfremdung diese Daten enthält[33]. Daß in § 12 Abs. 4 BDSG für den öffentlichen Bereich nicht auf § 31 BDSG verwiesen wird, muß als Versehen des Gesetzgebers gesehen werden. Ansonsten wären die Beschäftigten im öffentlichen Dienst gegenüber den Beschäftigten in der Privatwirtschaft benachteiligt[34].

Nach **§ 33 Abs. 2 Nr. 3 BDSG** entfällt die Benachrichtigung auch dann, wenn die Daten 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[35]).

Die Benachrichtigung kann nach **§ 33 Abs. 2 Nr. 4 BDSG** unterbleiben, wenn das Bekanntwerden der gespeicherten Daten dem Wohle des Bundes oder Landes Nachteile bereiten würde. So muß die zuständige öffentliche Stelle gegenüber der speichernden Stelle festgestellt haben, daß das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle eines Landes Nachteile bereiten würde. So kann es sich unter Umständen als notwendig erweisen, daß personenbezogene Daten auch gegenüber dem Betroffenen geheimgehalten werden müssen, wenn z. B. ein Mitarbeiter unter dem Verdacht geheimdienstlicher Tätigkeit steht[36]). Nach Lage der Dinge kommt eine solche Maßnahme allenfalls im Rahmen der Strafverfolgung in Betracht[37]).

Nach **§ 33 Abs. 2 Nr. 5 BDSG** muß der Betroffene nicht benachrichtigt werden, wenn die Daten in einer Datei gespeichert werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden. Gegen diese Regelung werden zu Recht schwerste Bedenken geltend gemacht[38]). So könnte bspw. eine Datei im Vorfeld wichtiger Entscheidungen wie Einstellungen oder Beförderungen erstellt und so zu kontrollierenden Verknüpfungen genutzt werden. „Ein ‚überwiegendes Allgemeininteresse' für eine solche Freistellung von den Kontrollrechten des einzelnen ist nicht ersichtlich; auch die Funktionsfähigkeit eines Unternehmens würde nicht leiden, wenn man – wie bisher – auf einen solchen Ausnahmetatbestand verzichten würde."[39]) Vor diesem Hintergrund ist die Ausnahmevorschrift der Nr. 5 restriktiv auszulegen.[40])

---

22) Vgl. Dörr/Schmidt (Fn. 19), § 33 Rn. 16.

23) Vgl. Simitis/Dammann/Mallmann/Reh (Simitis), Kommentar zum Bundesdatenschutzgesetz, 3. Aufl., Baden-Baden 1981, § 26 Rn. 6; Bergmann/Möhrle/Herb (Fn. 4), § 33 Rn. 34; Koch, Datenschutzhandbuch für die betriebliche Praxis, Freiburg im Breisgau, 1987, S. 101; Auernhammer (Fn. 8), § 33 Rn. 8.

24) Vgl. Bergmann/Möhrle/Herb (Fn. 4), § 33 Rn. 35 und Rn. 40.

25) Vgl. Bergmann/Möhrle/Herb (Fn. 4), § 33 Rn. 76.

26) Auernhammer (Fn. 8), § 33 Rn. 10.

27) Vgl. z. B. Wächter, Die Entbehrlichkeit der Benachrichtigung nach § 33 Abs. 2 Nr. 1 BDSG, CR 9/92, S. 558 ff; vgl. auch Ordemann/Schomerus/Gola (Fn 14) § 33 Anm. 6.1.

28) Vgl. Dörr/Schmidt (Fn. 19), § 33 Rn. 19; Simitis (Fn. 23), § 26 Rn. 16.

29) Vgl. Koch (Fn. 23), S. 154.

30) Vgl. Simitis (Fn. 23), § 26 Rn. 17.

31) Vgl. Däubler, Gläserne Belegschaften? 3. Aufl., Köln 1993, Rn. 264; Simitis (Fn. 23) § 26 Rn. 17.

32) Vgl. Ordemann/Schomerus/Gola (Fn. 14), § 33 Anm. 6.1.

33) Vgl. Däubler (Fn. 14), S. 477; vgl. auch Bergmann/Möhrle/Herb (Fn. 4), § 33 Rn. 110.

34) Vgl. hierzu Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum Bundesdatenschutzgesetz, 4. Aufl., 1992, § 12 Rn. 31.

35) Vgl. Däubler (Fn. 14), S. 477; Auernhammer (Fn. 8), § 33 Rn. 15.

36) Vgl. Ordemann/Schomerus/Gola (Fn. 14), § 33 Anm. 6.4.

37) Vgl. Däubler (Fn. 14), S. 477.

38) Vgl. Däubler (Fn. 14), S. 477; Bergmann/Möhrle/Herb (Fn. 4), § 33 Rn. 122; anderer Auffassung: Auernhammer (Fn. 8), § 33 Rn. 18; Schaffland/Wiltfang (Fn. 19), § 33 Rn. 72; Dörr/Schmidt (Fn. 19), § 33 Rn. 28.

39) Däubler (Fn. 14), S. 477; Auernhammer (Fn. 8) § 33 Anm. 18.

40) Vgl: Bergmann/Möhrle/Herb (Fn. 4), § 33 Rn. 122.

Nach **§ 33 Abs. 2 Nr. 6 a BDSG** kann die Benachrichtigung entfallen, wenn die Daten für eigene Zwecke gespeichert und aus allgemein zugänglichen Quellen entnommen sind. Zu den allgemein zugänglichen Quellen zählen insbesondere Printmedien (z. B. Zeitungen, Adreßbücher, Branchenverzeichnisse, Telefonbücher) sowie Hörfunk, Fernsehen, Filme und Videos. Diese Regelung ist in dieser Form 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 dies nicht die Befugnis, die Informationen zu speichern oder mit anderen personenbezogenen Daten zu verknüpfen.[41])

Nach **§ 33 Abs. 2 Nr. 6 b BDSG** kann eine Benachrichtigung schließlich entfallen, wenn die Benachrichtigung die Geschäftszwecke der speichernden Stelle erheblich gefährden würde. Eine Ausnahme soll dann gelten, wenn das Interesse an der Benachrichtigung die Gefährdung überwiegt. In bezug auf Beschäftigungsverhältnisse 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.[42])

Ein Verstoß gegen die Benachrichtigungspflicht ist gemäß § 44 Abs. 1 Nr. 3 BDSG bußgeldbewehrt. Wer den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt, begeht eine Ordnungswidrigkeit.[43])

In der Mehrzahl der Landesdatenschutzgesetze ist eine Benachrichtigungspflicht nicht vorgesehen. Dies wird u. a. damit begründet, daß die Daten direkt bei dem Betroffenen mit seiner Kenntnis erhoben werden müssen.

Da insbesondere vor dem Hintergrund der Ausnahmeregelungen zu befürchten steht, daß die Benachrichtigungspflicht in den Beschäftigungsverhältnissen „ins Leere läuft", sollte für das Arbeitsleben eine Regelung wie in **§ 18 Abs. 2 HDSG** angestrebt werden. Die hessische Verwaltung ist verpflichtet, bei der **erstmaligen Speicherung von personenbezogenen Daten** in einer automatisierten Datei die Betroffenen **schriftlich** davon zu **benachrichtigen** und dies unaufgefordert. Dabei ist nicht darauf abzustellen, ob der Betroffene auf andere Weise Kenntnis erlangt hat. Die Benachrichtigung, die schriftlich zu erfolgen hat, muß u. a. zu erkennen geben, welche Datenarten zu welchem Zweck wie lange gespeichert werden[44]).

5.3 Recht auf Auskunft gemäß § 34 BDSG

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

- die zu seiner Person gespeicherten Daten,
- die Herkunft,
- den oder die Empfänger,
- die Personen bzw. Stellen, an die seine Daten regelmäßig übermittelt werden für den Fall der automatisierten Datenverarbeitung.

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 definierte Begriff „personenbezogene Daten", denn er umfaßt über jede Einzelangabe hinaus auch Angaben über die gespeicherten Daten. So gehört zu den zur Person gespeicherten Daten auch die Bezeichnung der jeweiligen Dateien[45]). 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[46]). Gemeint sind externe Personen und Stellen, wobei auch die Adresse desjenigen, von dem die Daten stammen, anzugeben ist[47]). **„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[48]). Durch diese Regelungen werden das Recht auf Datenkorrektur über die speichernde Stelle hinaus bis in die gesamte Übermittlungskette erleichtert[49]).

Ferner ist dem Betroffenen der **Zweck der Speicherung** der Daten, mitzuteilen. „Die Rechtsgrundlage der Speicherung ist anders als nach dem § 18 Abs. 1 HDSG nicht ausdrücklich erfaßt. In vielen Fällen wird sich der ‚Zweck der Speicherung' allerdings nur unter Hinweis auf eine bestimmte Rechtsnorm erläutern lassen."[50]) Zu dem Zweck gehört in jedem Fall der allgemeine Verwendungszusammenhang der Daten, z. B. Lohn- und Gehaltsabrechnung, sowie auch die Angabe der eingesetzten Anwendungsprogramme[51]).

Im Falle der automatisierten Verarbeitung der Daten sind Angaben über die Personen und Stellen zu machen, an die die Daten **regelmäßig übermittelt** werden. Diese Pflicht besteht unabhängig davon, ob diese Angaben beim Arbeitgeber per EDV gespeichert sind. Voraussetzung ist jedoch, daß die Daten regelmäßig übermittelt werden. Eine regelmäßige Übermittlung liegt vor, wenn der Empfang der Daten in bestimmten Zeitabschnitten erfolgt, z. B. auch dann wenn alle zwei Jahre übermittelt wird[52]).

Das Auskunftsverlangen selbst 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. Abweichend vom bisherigen Recht ist nach § 34 Abs. 5 BDSG die Auskunft unentgeltlich.

Nach § 34 Abs. 4 BDSG gelten die in § 33 Abs. 2 Nr. 2 – Nr. 6 BDSG für die Benachrichtigungspflicht aufgestellten Ausnahmen auch in bezug auf eine Auskunftserteilung gemäß § 34 BDSG.

Die Landesdatenschutzgesetze enthalten für ein Auskunftsrecht fast identische Regelungen.

Dem Auskunftsrecht nach § 34 BDSG gehen gemäß § 1 Abs. 4 BDSG

---

41) Vgl. Däubler (Fn. 14), S. 477.

42) Vgl. Ordemann/Schomerus/Gola (Fn. 14), § 33 Anm. 6.7.

43) Vgl. Bergmann/Möhrle/Herb (Fn. 4), § 33 Rn. 151; Simitis (Fn. 23), § 26 Rn. 13; Koch (Fn. 23), S. 101.

44) Vgl. Schapper, Datenschutz und Datensicherung beim betrieblichen Einsatz von Personalcomputern, ArbuR 4/88, S. 102; ähnliche Regelungen wie das HDSG enthalten das Berliner Datenschutzgesetz und das Niedersächsische Datenschutzgesetz.

45) Vgl. Bergmann/Möhrle/Herb (Fn. 4), § 34 Rn. 38; HessVGH, Beschuß v. 17. 12. 1990, RDV 4/91, S. 188.

46) Vgl. Däubler (Fn. 14), S. 478; Tinnefeld/Ehmann (Fn. 3), S. 219.

47) Vgl. Bergmann/Möhrle/Herb (Fn. 4), § 34 Rn. 40.

48) Vgl. Bergmann/Möhrle/Herb (Fn. 4), § 34 Rn. 41.

49) Vgl. Tinnefeld/Ehmann (Fn. 3), S. 220.

50) Däubler (Fn. 31), Rn. 275.

51) Vgl. Däubler (Fn. 14), S. 478 mit weiteren Nachweisen; anderer Auffassung: Tinnefeld/Ehmann (Fn. 3), S. 219.

52) Vgl. Bergmann/Möhrle/Herb (Fn. 4), § 34 Rn. 50; Ordemann/Schomerus/Gola (Fn. 14), § 34 Anm. 2.5.

andere Rechtsvorschriften vor. Zu solchen Rechtsvorschriften (Spezialregelungen) gehören bspw. die Regelungen des § 90 Bundesbeamtengesetz (BBG), § 56 Beamtenrechtsrahmengesetz (BRRG) und § 13 Bundesangestelltentarifvertrag (BAT). Danach haben Beamte und Angestellte ein Recht auf Einsicht in die Personalakte. Diese Rechte verdrängen den § 34 BDSG jedoch nicht ganz, sondern nur soweit, wie eine Deckungsgleichheit besteht. Ansonsten kommt der § 34 BDSG zum Tragen[53]).

5.4 Recht auf Datenkorrektur nach § 35 BDSG

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) und
- Sperrung (§ 35 Abs. 3 und 4 BDSG).

5.4.1 Anspruch auf Berichtigung nach § 35 Abs. 1 BDSG

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 speichernde Stelle von sich aus verpflichtet, unrichtige Daten zu berichtigen[54]). Die Berichtigungspflicht besteht für unrichtige Daten, also für Daten, die mit der Realität nicht übereinstimmen[55]). Unrichtigkeit liegt jedoch nicht nur bei offenkundigen Fehlern, unrichtigen Adressen oder unrichtigen Geburtsnamen, sondern auch bei einem sogenannten Kontextverlust der Daten vor, der so gravierend ist, daß Fehlinterpretationen zumindest wahrscheinlich sind[56]). 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 des Beschäftigten[57]). 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[58]).

Eine Berichtigung kann erfolgen, indem

- ein falsches durch ein richtiges Datum ersetzt,
- ein Datum vervollständigt oder
- ein Datum ersatzlos gestrichen wird[59]).

Wurden Daten regelmäßig an Dritte weitergegeben, hat die speichernde Stelle diese gemäß § 35 Abs. 6 BDSG von der Berichtigung zu verständigen.

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[60]).

5.4.2 Recht auf Löschung nach § 35 Abs. 2 BDSG

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 bestimmter sensibler Daten nicht bewiesen werden kann oder
- die Daten nicht mehr erforderlich sind.

Eine **unzulässige Speicherung** liegt immer dann vor, wenn die Zulässigkeitsvoraussetzungen gemäß § 4 Abs. 1 BDSG nicht gegeben sind. Zu beachten ist zudem, daß die Daten vor der Speicherung auch rechtmäßig erhoben worden sein müssen. Hier kommt insbesondere § 13 BDSG zum Tragen. Nicht rechtmäßig erhoben sind die Daten auch dann, wenn das Fragerecht des Arbeitgebers überschritten wurde. Für den öffentlichen Dienst wird der Umfang der Datenerhebung zusätzlich durch das Recht auf gleichen Zugang zu jedem öffentlichen Amt aus Art. 33 GG begrenzt. Die Erhebung muß sich hier also im Rahmen der Kriterien der Eignung, Befähigung und fachlichen Leistung halten[61]). Zudem ist bei Verweigerung bestehender Mitbestimmungsrechte des Personalrats bei der Erhebung eine Speicherung unzulässig. Dies gilt in gleicher Weise bei einem Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Überwachungseinrichtungen (§ 75 Abs. 3 Nr. 17 BPersVG).

Da die Beweislast für die Zulässigkeit der Datenverarbeitung grundsätzlich bei der speichernden Stelle liegt, muß sie dem Betroffenen beweisen, daß kein Löschungsanspruch besteht[62]).

Besonders **sensible Daten**, nämlich über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen, 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[63]). 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[64]).

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 auf Daten von Beschäftigten bzw. ausgeschiedenen Arbeitnehmern beziehen.

5.4.3 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 werden drei Alternativen aufgestellt, bei denen die Daten nicht gelöscht werden dürfen bzw. müssen. So tritt an Stelle einer Löschung eine Sperrung, wenn

---

53) Vgl. Däubler (Fn. 31), Rn. 282 ff.; Ordemann/Schomerus/Gola (Fn. 14), § 1 Anm. 7.1.

54) Vgl. Simitis (Fn. 23), § 27 Rn. 7; Dörr/Schmidt (Fn. 19), § 35 Rn. 1; Ordemann/Schomerus/Gola (Fn. 14), § 35 Anm. 2.1; Bergmann/Möhrle/Herb (Fn. 4), § 35 Rn. 29.

55) Vgl. Simitis (Fn. 23), § 14 Rn. 7.

56) Vgl. Simitis (Fn. 23), § 14 Rn. 9; Däubler (Fn. 14), S. 480; Ordemann/Schomerus/Gola (Fn. 14), § 35 Anm. 2.1.

57) Vgl. Bergmann/Möhrle/Herb (Fn. 4), § 35 Rn. 30; Wohlgemuth (Fn. 4), S. 185 f.; Däubler (Fn. 14), S. 480.

58) Vgl. Ordemann/Schomerus/Gola (Fn. 14), § 35 Anm. 2.1; Gola/Wronka (Fn. 8), S. 182.

59) Vgl. Tinnefeld/Ehmann (Fn. 3), S. 221

60) Vgl. Ordemann/Schomerus/Gola (Fn. 14), § 35 Anm. 2.1.

61) Vgl. ausführlich Stange (Fn. 8), S. 175 ff.

62) Vgl. Bergmann/Möhrle/Herb (Fn. 4), § 35 Rn. 61.

63) Vgl. Stange (Fn. 8), S. 175 ff.

64) Vgl. Däubler (Fn. 14), S. 481.

- 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 § 34 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 speichernde 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.

Die Landesdatenschutzgesetze sehen in bezug auf Berichtigung, Löschung und Sperrung ähnliche Regelungen vor.

In bezug auf Berichtigung, Löschung und Sperrung nach § 35 BDSG gehen gemäß § 1 Abs. 4 BDSG andere Rechtsvorschriften vor. Zu diesen Rechtsvorschriften gehören bspw. § 13 Abs. 2 BAT, § 90b BBG und § 56 BRRG. Danach muß der Beamte zu Beschwerden, Behauptungen und Bewertungen, die für ihn ungünstig sind oder nachteilig werden können, vor deren Aufnahme in die Personalakte gehört werden. Zudem ist seine Äußerung zur Personalakte zu nehmen. Unterlagen über Beschwerden, Behauptungen und Bewertungen sind mit Zustimmung des Beamten unverzüglich aus der Personalakte zu entfernen und zu vernichten, falls sie sich als unbegründet oder falsch erwiesen haben (§§ 90e BBG, 56e BRRG). Nach § 13 Abs. 2 BAT muß der Angestellte über Beschwerden und Behauptungen tatsächlicher Art, die für ihn ungünstig sind oder ihm nachteilig werden können, vor Aufnahme in seine Personalakte gehört werden. Seine Äußerungen sind zu den Personalakten zu nehmen. Diese Spezialregelungen gehen den Regelungen des § 35 BDSG jedoch nur soweit vor, wie eine Deckungsgleichheit der Ansprüche besteht. Ansonsten kommt § 35 BDSG zum Tragen.

5.5 Schadensersatz gemäß § 7 BDSG

Das BDSG normiert einen Schadensersatzanspruch bei unzulässiger oder unrichtiger automatisierter Verarbeitung personenbezogener Daten, durch die der Betroffene in seinen schutzwürdigen Belangen beeinträchtigt wird. Das BDSG unterscheidet, ob der Schadensersatz durch eine nicht-öffentliche Stelle (§ 8 BDSG) oder eine öffentliche Stelle (§ 7 BDSG) zu leisten ist. Im Rahmen dieser Abhandlung ist lediglich § 7 BDSG von Bedeutung.

Um den Ersatz von Schaden zu erleichtern, der den Betroffenen durch unrichtige oder unzulässige Verarbeitung seiner personenbezogene Daten durch eine öffentliche Stelle entstanden ist, hat der Gesetzgeber – nach dem Vorbild der weitgehend wörtlich übernommenen § 20 Abs. 1 HDSG, § 20 Abs. 1 DSG-NW – nunmehr eine umfassende Gefährdungshaftung festgelegt[65]). Mit dem Gefährdungshaftungstatbestand, der kein Verschulden der speichernden Stelle vorsieht, soll der Tatsache Rechnung getragen werden, daß die Tatbestände der üblichen Verschuldenshaftung den Besonderheiten der modernen Datenverarbeitung nicht gerecht werden. „In Anbetracht der komplexen, für außenstehende Dritte kaum nachvollziehbaren Vorgänge bei der automatisierten Datenverarbeitung kann es dem Betroffenen nicht zugemutet werden, dem Betreiber der Anlage ein Verschulden nachweisen zu müssen."[66])

Unzulässig ist die Datenverarbeitung dann, wenn sie auch nur in einer der Verarbeitungsphasen, wie Speichern, Verändern, Übermittlen, Sperren oder Löschen nicht durch die Zulässigkeitsvoraussetzungen nach § 4 Abs. 1 BDSG abgedeckt ist[67]). Unrichtig ist die Datenverarbeitung dann, wenn unrichtige Daten richtig verarbeitet werden oder richtige Daten unrichtig verarbeitet werden. Liegt die schädigende Handlung ausschließlich in einem Programmfehler oder in einem technischen Defekt, so liegt eine unrichtige Datenverarbeitung vor, so daß auch hier ein Schadensersatzanspruch besteht[68]). Zwischen unzulässiger und unrichtiger Datenverarbeitung und dem den Betroffenen zugefügten Schaden muß ein ursächlicher Kausalzusammenhang bestehen. Der Schadensanspruch kann als höchstpersönliches Recht nur von den Betroffenen selbst geltend gemacht werden[69]). In § 7 Abs. 3 BDSG ist die Höchstgrenze für materielle und immaterielle Schäden auf 250000 DM festgelegt.

Die Reichweite der Haftungsnormen der Landesdatenschutzgesetze ist uneinheitlich. So sieht § 17 BlnDSG eine in der Höhe grundsätzlich unbegrenzten Schadensausgleich vor. In Hamburg, Hessen, Nordrhein-Westfalen erkennen die Gesetze z. B. grundsätzlich den materiellen Schaden bis zu 500000 DM je Betroffenen und je schadensstiftenden Ereignis an, wohingegen im Bremischen Datenschutzgesetz eine entsprechende Regelung fehlt.

Bruno Schierbaum/
Eberhard Kiesche,
BTQ Niedersachsen – Beratungsstelle für Technologiefolgen und Qualifizierung

65) Vgl. Auernhammer, Bundesdatenschutzgesetz vom 20. Dezember 1990, Köln, 1992, § 7 Rn. 5.

66) BT-Drs. 11/4306, S. 41; zitiert nach Auernhammer (Fn. 65), § 7 Rn. 2; vgl. auch Bergmann/Möhrle/Herb (Fn. 4) § 7 Rn. 5 f.

67) Vgl. Auernhammer (Fn. 8), § 7 Rn. 5.

68) Vgl. Lübking (Fn. 8), S. 114; Ordemann/Schomerus/Gola (Fn. 14), § 7 Rn. 3.4.

69) Vgl. Ordemann/Schomerus/Gola (Fn. 14), § 7 Anm. 3.2.