Daten- und Persönlichkeitsschutz im Arbeitsverhältnis

Praxishandbuch zum Arbeitnehmerdatenschutz

von

Prof. Dr. Stephan Weth, Prof. Dr. Maximilian Herberger, Dr. Michael Wächter, Dr. Ulrich Baumgartner, Thomas Breyer, Dominic Broy, Dr. Philipp Byers, Prof. Franz Josef Düwell, Dr. Jan Fritz Geiger, Yvonne Gutting, Ines M. Hassemer, Dennis Heinson, Dr. Stefan Kramer, Dr. Hendrik Schöttle, Katharina Sicking, Christian Willert

1. Auflage

Thematische Gliederung:

Arbeitsvertrag, Arbeitsentgelt

Verlag C.H. Beck München 2014

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 63194 8

lerdings ist im Einzelfall auch genau abzuwägen, ob § 32 BDSG oder § 28 1 Nr. 2 BDSG anzuwenden ist, wenn es um die **Erfüllung unternehmerischer Sorgfalt** geht, bei deren Wahrnehmung auch kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Bei der Bewertung der rechtlichen Situation ist allerdings zu beachten, dass auch eine zulässige Datenverarbeitung Persönlichkeitsrechte von Arbeitnehmern beeinträchtigen kann.[11]

7 Compliance ist damit ein Organisationsmodell für Prozesse und Systeme, welche primär orientiert sind an der Einhaltung interner Unternehmensprozesse. Das Spannungsfeld zum Arbeitnehmerdatenschutz besteht hierbei darin, dass zur Umsetzung von Compliance die Wahrnehmung von **Kontroll- und Überwachungspflichten** erforderlich ist, die eine Vielzahl von Unternehmens-, und auch Personalprozessen (zB zur Reisegenehmigung und Reisekostenerstattung) betreffen können. Compliance erstreckt sich hierbei nicht nur auf die Beachtung rechtlicher Vorgaben durch die Unternehmensleitung, sondern auch auf die Handhabung von Unternehmensaufgaben durch Arbeitnehmer selbst.

8 Neben den Pflichten der verantwortlichen Stelle, die wahrzunehmen sind, sind auch das **Selbstdenken**[12] und die Selbstkontrolle der Betroffenen zum Umgang mit ihren über sie selbst und auch über andere generierten Daten von Bedeutung. Datenschutz bedarf in Unternehmen zu seiner **Etablierung insofern eines Datenschutzbewusstseins** aller an IT und Kommunikation Beteiligten. Schutz von Unternehmensgütern sowie individueller Rechtsschutz und soziale Bindung des Einzelnen setzen zu seiner Gewährleistung nicht nur die Übernahme von Verantwortung für Datenschutz des Unternehmens voraus, sondern auch die Mündigkeit von Betroffenen. Persönlichkeitsrecht setzt – im Rahmen einer Compliance von Unternehmen – auch auf Eigenverantwortlichkeit jedes einzelnen Akteurs.

9 Je mehr in Unternehmen Mitarbeiter ihre Anträge (zB auf Reisegenehmigung) in Tools, Anwendungen und IT-gestützten Unternehmensprozessen eigenständig stellen und auch die Dokumentationen ihrer Geschäftsvorgänge (zB Opportunities im Vertrieb) in Vertriebsdatenbanken eigenständig wahrnehmen, um so mehr erstreckt sich die **Integrität von Unternehmen** auch auf die Integrität der Handlungen von Mitarbeitern. Dies betrifft im Besonderen Mitarbeiter mit direktem Lieferanten- (Einkauf) oder Kundenkontakt (Vertrieb und Beratung). Dennoch bleibt die primäre Verantwortung für Integrität und Compliance, dh die **Einhaltung gesetzeskonformen Verhaltens** sowie betriebswirtschaftlicher Standards bei der Unternehmensleitung. Insofern bedarf es einer Kontrolle.

10 Compliance steht im Kontext der Verantwortung der Unternehmensleitung. Hierbei geht es um **Verantwortlichkeit „aus" Leitung** (Corporate Governance). In Unternehmen wird hierbei zwischen Management/Ownership (Leitung, Prozessverantwortlichkeit) und Control/Accounting (Kontrolle/Rechnungswesen) unterschieden. Im Deutschen Corporate Governance Codex ist unter Ziffer 4.1.3. geregelt, dass der **Vorstand** für die Einhaltung der gesetzlichen Bestimmungen sowie der unternehmensinternen Richtlinien zu sorgen hat. Damit unterliegen Unternehmen einem **Risiko-Management.** Eine sorgfältige Geschäftsführung (vgl. §§ 93 I, 76 I AktG) erfordert damit ein Überwachungssystem. Auch der Geschäftsführer einer GmbH muss erkennbaren Risiken Rechnung tragen, auch wenn § 43 I GmbHG keine dem § 93

---

[11] Vgl. dazu auch *Gola/Schomerus,* § 13 Rn. 3.
[12] *Hufen,* JuS 2013, 1 ff. (5).

I 2 AktG entsprechende Regelung enthält, wonach das Handeln zum Wohle der Gesellschaft auf angemessenen Informationen beruhen muss. Der GmbH-Geschäftsführer muss Entscheidungen jedenfalls sorgfältig vorbereiten.

11 Der Vorstand einer Aktiengesellschaft muss nach § 91 II AktG geeignete Maßnahmen treffen, insbesondere ein Überwachungssystem einrichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Nach § 161 I 1 AktG erklären Vorstand und Aufsichtsrat einer börsennotierten Gesellschaft jährlich, dass den vom Bundesministerium der Justiz im amtlichen Teil des Bundesanzeigers bekannt gemachten Empfehlungen der „Regierungskommission Deutscher Corporate Governance Kodex" entsprochen wurde und wird oder welche Empfehlungen nicht angewendet wurden oder werden und warum nicht.

12 Nutzt ein Unternehmen den amerikanischen **Kapitalmarkt,** so unterliegt es der US-Börsenaufsichtsbehörde für die Kontrolle des Wertpapierhandels in den Vereinigten Staaten (United States Securities and Exchange Commission – **SEC**). Im Arbeitnehmerdatenschutz ist Compliance im Wesentlichen für die betriebswirtschaftliche Sichtweise des Owners von IT-Anwendungen und die Etablierung von Managementverantwortung von Bedeutung. Sonderthemen der Compliance im Kapitalmarkt verdeutlichen allerdings den heutigen Stellenwert von Compliance. So muss ein Wertpapierdienstleistungsunternehmen organisatorische Pflichten nach § 25a I und IV des Kreditwesengesetzes (KWG) einhalten (vgl. § 33 Gesetz über den Wertpapierhandel – WpHG). Für Compliance sind im Besonderen auch Risiken relevant, die sich in der Vergangenheit realisiert haben. Insofern hatten auch die sog. Datenskandale die Etablierung der Compliance im Arbeitnehmerdatenschutz zur Folge.[13]

13 Aus dem Dargestellten wird ersichtlich, dass mit der Schaffung der Vorschrift des § 32 BDSG vom Gesetzgeber nicht intendiert wurde, Pflichtverstöße im Arbeitsverhältnis bzw. den Unrechtsgehalt von Straftaten zu legitimieren.[14] Vielmehr sind bei der **Umsetzung von Compliance** Missstände konsequent aufzudecken. Allerdings unter Beachtung einer Abwägung von Datenermittlungsbefugnissen und Individualrechten. Insofern darf die Ermittlung von beschäftigtenbezogenen Daten sowie auch die Herausgabe von Daten nicht gegen das **Übermaßverbot** verstoßen.[15] Compliance auf dem Gebiet von Datenschutzverstößen bedeutet insofern, den Schutz der Privatsphäre in einem Gesamtrechtszusammenhang zu sehen. Insofern wird bei der rechtlichen Prüfung von Privatsphäreaspekten zu berücksichtigen sein, dass Arbeitnehmer, die im Unternehmen eine Position innehaben, eine Aufgabenstellung wahrnehmen oder eine Jobrolle ausfüllen, nicht nur Rechte haben, sondern ihnen auch Verantwortung zugerechnet werden kann. Arbeitnehmer sind insofern auch **„Sozialperson".**[16]

14 Rechtspolitisch wird bei der Schaffung eines künftigen **Beschäftigtendatenschutzgesetzes** erwartet, dass die berechtigten Interessen von Unternehmen und die schutzwürdigen Interessen der Beschäftigten – auch im Hinblick auf eine Verantwortungszurechnung von Arbeitgeber und Arbeitnehmer – präziser gefasst werden.[17] Im Moment geht es allerdings darum, die „Messbarkeit"[18] der geltenden datenschutzge-

---

[13] *Thüsing,* Rn. 6.
[14] Vgl. dazu *Hamm*, NJW 2010, 1332 ff. (1336).
[15] Vgl. zum Gegenstand des Übermaßverbotes *Michael/Morlok,* Rn. 612 ff.
[16] Der Terminus stammt von *Philipps,* Zur Ontologie der sozialen Rolle, 1963, S. 13. Die Rolle eines Menschen – als Bürger – sowie seiner Aktivitäten – als Vertragspartner – bestimmt insofern das Maß seiner Pflichten auch als Arbeitnehmer mit.
[17] Vgl. dazu z. B. *Däubler,* Rn. 948.
[18] Zu diesem methodischen Ansatz *Ballweg,* S. 51 ff. (52).

setzlichen Regelungsvorgaben zu erhöhen und eine angemessene Lösung zu erreichen. Ferner geht es um die Herstellung einer „Intersubjektivität“[19] von Rechtsanwendungsergebnissen. Insofern endet jeder Absatz in diesem Kapitel mit einem **Fallbeispiel,** welches die situative Findung einer datenschutzgerechten Lösung für Unternehmen und Arbeitnehmer exemplifizieren soll.

b) Funktion der Internen Revision und Datensicherheit

Die Interne Revision ist ein Kontrollinstrument, mit dem sich die Unternehmensleitung von der Einhaltung unternehmensinterner Vorgaben sowie von rechtlichen Regelungen zur Einhaltung der **Ordnungsmäßigkeit von Geschäftsvorgängen** überzeugt. Die Revision muss neben der Ordnungsmäßigkeit auch Aspekte der Wirtschaftlichkeit, Zweckmäßigkeit und Sicherheit von Geschäftsvorgängen überprüfen. Nicht zur Aufgabe der Revision gehören regelmäßig personenbezogene Auswertungen. Die Revision ist insofern eine Überwachungsinstanz, welche sich mit der Korrektheit von Geschäftsvorgängen befasst. Zu beachten sind hierbei im Besonderen die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme **(GoBS).** **15**

Buchführung bezeichnet die in Zahlenwerten vorgenommene Aufzeichnung der Geschäftsvorgänge in einem Unternehmen. Die Buchführung muss so beschaffen sein, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle sowie über die Lage des Unternehmens vermitteln kann (§ 238 I 2 HGB). Buchführungspflichten haben hierbei zur Voraussetzung, dass die entsprechenden Daten auch erfasst und dokumentiert werden.[20] **16**

Analyseobjekt der Revision ist insofern die Einhaltung vorgeschriebener Prozesse. Dazu gehören die ordnungsgemäße Abbildung von Geschäftsvorgängen und die korrekte Gehaltsabrechnung. Dies betrifft auch die Einhaltung von Richtlinien zur Reisekostenabrechnung. Dies bedeutet, dass alle relevanten Informationen – im Besonderen Belege – sorgfältig, korrekt und vollständig erfasst werden müssen. Die rechtliche Grundlage für die Erstellung einer Verfahrensdokumentation ergibt sich aus § 239 HGB (Führung der Handelsbücher). **17**

Aus der Vorschrift des § 257 HGB ergeben sich die Aufbewahrungsfristen. Danach sind zB Belege für Buchungen und Jahresabschlüsse 10 Jahre aufzubewahren. Empfangene Handelsbriefe jeweils 6 Jahre. Es besteht nach § 238 HGB insgesamt eine Verpflichtung, Bücher zu führen und in diesen die Handelsgeschäfte nach den Grundsätzen ordnungsmäßiger Buchführung ersichtlich zu machen. **18**

In § 147 (Ordnungsvorschriften für die Aufbewahrung von Unterlagen) und § 147a AO (Vorschriften für die Aufbewahrung von Aufzeichnungen und Unterlagen bestimmter Steuerpflichtiger) sind die Regelungen im Hinblick auf **Steuerpflichten** festgelegt. Dazu ist nach § 147 I AO vorgeschrieben, dass zB Buchungsbelege und Geschäftsbriefe geordnet aufzubewahren sind. Die Revision darf für die Erfüllung der genannten Sorgfaltspflicht als **Unterstützungsfunktion der Unternehmensleitung** die aufbewahrten Informationen und Unterlagen prüfen, dh erheben. Die Datenspeicherung und Nutzung der Informationen darf indes nur für den Erhebungszweck der Revisionsprüfung erfolgen (§ 28 I 2 BDSG). **19**

Zur Kontrolle der Einhaltung von Vorschriften zur Compliance dient die **Datenanalyse.** Grundlegende Annahme der Datenanalyse ist es, dass Regelübertretungen und -verstöße ihre Spuren in digitalen Datenbeständen hinterlassen. Aber auch regel- **20**

---

[19] *Ballweg,* S. 51 ff. (54); vgl. ferner *Popper,* S. 21 ff.

[20] *Schneider,* Kap. B Rn. 1; vgl. dazu auch Simitis/*Sokol,* § 4 Rn. 13.

konforme Transaktionen können Auffälligkeiten aufweisen. Zulässige Stichprobenprüfungen sind hierbei der Analyse massenhafter Daten, zB der Daten aller Geschäftsabschlüsse in einem Geschäftsjahr, gegenüber zu stellen. Mit der Analyse massenhafter Daten sollte restriktiv umgegangen werden. Die Analyse sollte für beide Verfahren (Stichprobe, Massenverfahren) immer durch festgelegte Kriterien erfolgen, welche risikoorientierte Fragestellungen im Hinblick auf den Beschäftigtendatenschutz berücksichtigen. Es werden vor diesem Hintergrund dann nur Datensätze herausgefiltert, die auf Regelverstöße bzw. Abweichungen hindeuten.

21 Die Interne Revision muss Aspekte der Wirtschaftlichkeit, Zweckmäßigkeit, Sicherheit und **Ordnungsmäßigkeit von Geschäftsvorgängen** überprüfen. Die Revision ist eine Überwachungsinstanz, welche insofern schwerpunktmäßig das Kriterium der Ordnungsmäßigkeit von Geschäftsvorgängen prüft. Prüfen und Kontrollieren betrifft die Erhebung und Verarbeitung von Informationen. Die Vorgehensweise der Internen Revision erfordert insofern die Beschreibung der Auswertungszwecke. Untersuchungskriterien und betroffene Dateien sind zu nennen. Problematisch ist insofern die Heranziehung von E-Mails als geschäftlicher Korrespondenz, soweit ein Mischbetrieb von geschäftlichen und privaten E-Mails im Unternehmen zugelassen wird. Hier ist auf den **Betreff,** dh das Subjekt zu achten, ob eine E-Mail als privat einzustufen ist. Nur geschäftliche Briefe sind als Analyseobjekt erforderlich.

22 Arbeitnehmer haben heute im Hinblick auf den Beschäftigtendatenschutz auch eine **Mitwirkungspflicht,** Informationen entsprechend zu kennzeichnen, auf deren Privatheit sie vertrauen möchten. Einschränkungen ergeben sich ferner bei geschlossenen Briefen und solchen, die als Privatbrief (Persönlich) kategorisiert sind.[21] Ebenso, wenn Briefe in einem geschlossenen Behältnis aufbewahrt werden. Die Datenanalyse von Kundendaten (zB Adress- und Kontoänderungen) ist zulässig, wenn das schutzwürdige Interesse der Betroffenen nicht nach § 28 I Nr. 2 BDSG überwiegt. Die Datenanalyse von Lieferantendaten sind grundsätzlich als Geschäftsdaten einzustufen. Sie sind in der **Sphäre des Unternehmens.**

23 Ein weiteres Feld ist die **Interne Revision und Datensicherheit.** Von Bedeutung ist hierbei auch das Informationssicherheitsmanagementsystem ISO 27001 als Maßstab für Qualität.[22] Aus dem Prozessverständnis ISO/IEC 27001 lassen sich folgende Ziele und Ansätze für ein Information Security Management ableiten. Hieraus ergibt sich eine Definition der **Information Security-Anforderungen** einer Organisation und die daraus abgeleitete Etablierung geeigneter Richtlinien und Ziele für Informationssicherheit. Es geht um die Implementierung und Etablierung von Kontrollen, um Risiken im Hinblick auf die Informationssicherheit im Unternehmen zu begegnen. Hinzu kommt das Monitoring und Reviewing der Effektivität des Information Security Management Systems. Und hierbei geht es um eine kontinuierliche Verbesserung basierend auf objektiven Indikatoren zur Verbesserung von Qualität.[23]

24 Auf internationaler Ebene spielen **Global Privacy Standards** eine Rolle, deren zentraler Begriff **Accountability** ist. Die zentrale Bedeutung liegt hierbei darin, dass Accountability den Aspekt der Verantwortung und Zurechenbarkeit mit dem Management-Aspekt der persönlichen Berechenbarkeit verbindet. Und dies ist entscheidend für die IT-Compliance, deren rechtliche Vorgaben nach §§ 5, 9 und 31 BDSG entlang der Prozessketten und Verantwortlichkeiten proaktiv, präventiv und fair umzusetzen

---

[21] *Wächter,* Datenschutz, Rn. 973.
[22] Vgl. zum Ansatz des Qualitätsmanagements *Wächter,* S. 111 ff.
[23] *Wächter,* Datenschutz, Rn. 146 ff.

sind. Privacy by Design adressiert hierbei Regeln eines effizienten Datenschutzes. Zentraler Ansatzpunkt ist im Arbeitnehmerdatenschutz nach Einführung des § 32 II BDSG das Thema der **End-to-End-Security,** welche Datenschutz und Datensicherheit über den gesamten Prozess der Datenverarbeitung betrachtet. Und dies auch gerade beim Medienwechsel von Papier (Akten) zu IT (Datenverarbeitung) und umgekehrt. Gerade der Wechsel von Trägermedien führt im Umgang mit Information zu Schwachstellen der Informationssicherheit.

Die Handhabung von Arbeitnehmerdatenschutz muss auf ein Konzept der Implementierung und Kontrolle von Datenschutz zielen, welches den gesetzlichen Anforderungen gerecht wird. Datenschutz bleibt dabei allerdings unter **betriebswirtschaftlicher Perspektive** integraler Bestandteil von Unternehmensprozessen und unternehmerischer Integrität. Applikationen, Kontent (Dateninhalte) und Prozesse werden in Unternehmen zunehmend integriert. Datenschutz ist damit Teil der Steuerung von Arbeits- und Geschäftsprozessen, denen entsprechende Rechtspositionen der Betroffenen gegenüber stehen. Dies macht auch die heutige **Komplexität** der Umsetzung von Datsenschutz und Datensicherheit aus. **25**

IT-Compliance im Arbeitnehmerdatenschutz kann der Umsetzung eines effizienten Datenschutzes dienen, indem gesetzeskonformes Handeln gewährleistet und Datenschutzverstössen vorgebeugt wird. Das Kriterium der Erforderlichkeit der Verarbeitung von Arbeitnehmerdaten nach § 32 I 1 BDSG muss hierbei in jedem Einzelfall beachtet werden. Im Rahmen der Zweckbestimmung des Beschäftigungsverhältnisses ist der **Gegenstand von IT-Verfahren** festzulegen. Für die Durchführung von Beschäftigungsverhältnissen sind die Funktionalitäten von IT-Systemen, die Kategorien der personenbezogenen Daten, deren Speicherdauer sowie Löschungsanforderungen zu betrachten, ob diese auch dem Grundsatz der Erforderlichkeit nach § 32 I 1 BDSG entsprechen. **26**

Ein moderner Ansatz, Arbeitnehmerdatenschutz zu etablieren, ist insofern das Thema der Technikgestaltung, um Datensicherheit und die materiellen Zulässigkeiten in ein Zusammenspiel zu setzen. Technikgestaltung sieht hierbei vor, Risiken bereits im Vorfeld einer Datenverarbeitung zu vermeiden oder zu minimieren **(Privacy by Design).**[24] Eine moderne Praxis des Arbeitnehmerdatenschutzes muss insofern neben der Transparenz, welche die Information des Einzelnen zur Verarbeitung seiner Daten betrifft, die Technikgestaltung in dieses Gesamtkonzept des Datenschutzes mit einbeziehen. Und hierzu gehört im Arbeitnehmerdatenschutz als weiterer Punkt in ganz zentraler Weise die Umsetzung der **Verschlüsselungsanforderung** der Anlage S. 2 zu § 9 S. 1 BDSG.[25] **27**

Hinzu kommt, dass bei der Verarbeitung von Beschäftigtendaten die Aspekte der **Schnittstellen zu anderen IT-Systemen,** die Festlegung der Daten- und Programmverantwortung (Systemowner), der Zugriffsberechtigungen (Job-Rolle, Need-to-know) sowie der vorgesehenen Reports aus einer Anwendung zu beachten sind. Der Systemowner, die Systemadministratoren sowie die für den Betrieb des IT-Systems zuständigen Beschäftigten sind nach § 5 BDSG auf das Datengeheminis zu verpflichten. IT-Compliance im Hinblick auf Datensicherheit ist damit wesentlicher Bestandteil auch der Einhaltung von Vorgaben zum Arbeitnehmerdatenschutz. **28**

---

[24] *Reding,* ZD 2011, 1 f. (2); vgl. zu diesem Konzept im Detail Peters/Kersten/Wolfenstetter/*Niemann/Scholz,* S. 109 ff.

[25] Instruktiv dazu Simitis/*Ernestus,* § 9 Rn. 164 ff.; s. ferner auch Taeger/Gabel/*Schultze-Melling,* § 9 Rn. 83 ff.

c) Fallbeispiel zur Revision bei der Kfz-Hauptuntersuchung

29 Die Aufgabenstellung der Internen Revision ist für die Einhaltung von Rechtsmäßigkeitsanforderungen von wesentlicher Bedeutung. Die Konflikte zum Datenschutzrecht sollen vorliegend am Fallbeispiel aus dem Geschäftsfeld einer Sachverständigenorganisation verdeutlicht werden, die technische Dienstleistungen auf dem Gebiet der Fahrzeugprüfungen nach der Straßenverkehrszulassungsordnung (StVZO) vornimmt (Prüftätigkeit). Das Beispiel ist deshalb so interessant, weil bei der Tätigkeit der Internen Revision ein augenscheinlicher Bezug zu beschäftigtenbezogenen Daten im Arbeitsverhältnis gegeben ist. Denn die Anforderungen der technischen Sicherheit betreffen hierbei auch die Unternehmensaufgabe der **Überprüfung von Prüfingenieuren** bei Prüftätigkeiten.

30 Im Rahmen der Internen Revision muss an Hand des **Prüfberichts** und dem verantwortlichen Prüfingenieur überprüft werden, ob die Prüfergebnisse fachlich richtig sind und die Vergabe einer Kfz-Plakette rechtmäßig erfolgt ist. Die Ergebnisse der **Hauptuntersuchung** (HU) sind hier dem Prüfbericht zu entnehmen. Da mit der Kontrolle des Prüfberichts nicht ersichtlich wird, ob das Prüfergebnis auch dem technischen Zustand des geprüften Fahrzeugs entspricht, kann es eine Möglichkeit sein, die Qualität der Arbeit von Prüfingenieuren durch den **Einsatz von Detektiven** zu überprüfen, die mit einem Fahrzeug mit erheblichen technischen Mängeln zu einer Hauptuntersuchung vorfahren. Damit kann dann unmittelbar festgestellt werden, ob der Prüfingenieur die vorhandenen Mängel fachlich korrekt festgestellt.

31 Dies verdeutlicht, dass die Revision die Untersuchung von Sachverhalten und Vorgängen auf ihre Ordnungsmäßigkeit und Richtigkeit hin beinhaltet. Die Interne Revision (Innenrevision) erfolgt dabei durch Mitarbeiter des Unternehmens. Aufgabenstellung der Internen Revision ist bei der Durchführung von Hauptuntersuchungen, ein internes Kontrollsystem für **Unternehmensrisiken** – hier zB der Wegfall der Voraussetzungen für die Anerkennung als Überwachungsorganisation – zu etablieren. Die Datenerhebung der Kfz-Daten muss hierbei datenschutzkonform erfolgen.[26] Ferner muss aber auch der Datenschutz und das Persönlichkeitsrecht der Prüfer bei der Revision ihrer Tätigkeit im Rahmen des Arbeitnehmerdatenschutzes beachtet werden.

32 Kernaufgabe der Internen Revision ist die Etablierung und Überprüfung der Ordnungsgemäßheit der Durchführung von Vorgängen und Aufgabenstellungen im Unternehmen an Hand geltender Gesetzen sowie unternehmensinterner Richtlinien. Zielsetzung hierbei ist der Schutz des Unternehmens sowie die Einhaltung von Qualitätsmaßstäben, welche zum rechtmäßigen Handeln des Unternehmens erforderlich sind. Da zu den Hauptaufgaben einer Sachverständigenorganisation die periodische **Überwachung von Kraftfahrzeugen** (Hauptuntersuchung, Abgasuntersuchung) gehört, muss gewährleistet sein, dass sich die geprüften Fahrzeuge nach der Straßenverkehrs-Zulassungs-Ordnung (StVZO) in einem verkehrssicheren Zustand befinden. Denn dies wiederum ist die Zielsetzung der HU.

33 Bei der Durchführung der HU hat der amtlich anerkannte Sachverständige oder Prüfer für den Kraftfahrzeugverkehr oder der von einer amtlich anerkannten Überwachungsorganisation betraute Prüfingenieur die Einhaltung der für diese Untersuchung geltenden Vorschriften des § 29 StVZO und der Anlage VIII beim Fahrzeug zu überprüfen. Bei der Durchführung der Untersuchung eines Fahrzeugs ist nicht nur sicher

---

[26] Vgl. zur Erhebung und Verarbeitung personenbezogener Daten im Rahmen der Hauptuntersuchung *Wächter,* DuD 1993, 391 ff.

zu stellen, dass der Sachverständige oder Prüfingenieur seine Arbeit nach den erforderlichen Qualitätsmaßstäben erbringt, sondern es geht auch darum, dass die **Ergebnisse der Hauptuntersuchung** überprüft werden.

34 Der Prüfingenieur wird im Bericht durch die Nummer seines persönlichen Prüfstempels identifiziert. Die Prüfberichte werden von der Sachverständigenorganisation entsprechend der Prüfstempelnummer – und auch der Personalkennziffer (Personalnummer) des Mitarbeiters – ausgewertet.[27] Im diesem Zug der Arbeit der Innenrevision werden auch die personenbezogenen Daten an Hand der erfassten **Prüfstempelnummer des Ingenieurs** verarbeitet, um dessen Tätigkeit zu überprüfen. Hierzu gehören auch der Ort und die Häufigkeit von Fahrzeug-Prüfungen durch den Prüfingenieur. Ist ein Prüfingenieur zB an einer Niederlassung in Süddeutschland angestellt und erfolgen von diesem Prüfingenieur gehäuft Prüfungen von Fahrzeugen mit einem bestimmten Fahrzeugkennzeichen aus Norddeutschland, so kann der Verdacht entstehen, dass ortsfremde Fahrzeuge unberechtigerweise und systematisch mit einer Prüfplakette versorgt werden.

35 Vor diesem Hintergrund hat die Interne Revision Zugriff auf Geschäftsdaten und auch auf Arbeitnehmerdaten. Eine enge Verknüpfung der Prüfdaten des Prüfingenieurs mit dem Arbeitsverhältnis ergibt sich auch daraus, dass dieser als angestellter Prüfingenieur arbeitsvertraglich in der Regel verpflichtet wird, die Hauptuntersuchung auch für sein Privatfahrzeug kostenfrei bei seiner Prüforganisation durchführen zu lassen.[28] Dies belegt – auch in diesem Geschäftsfeld – die enge Verknüpfung von geschäftlichen und privaten Daten.

36 Im Rahmen der Internen Revision ist hierbei in besonderer Weise auf **nichttechnische Formen der Kontrolle** hinzuweisen. Der Arbeitgeber kann grundsätzlich die Arbeitsleistung von Mitarbeitern kontrollieren. Eine Rückfrage zu Arbeitsergebnissen bei einzelnen Mitarbeitern verstößt – ebenso wenig wie die Überprüfung der allgemeinen Dienstleistungsqualität im Unternehmen – nicht gegen Anforderungen des § 32 BDSG.[29] Hat der Prüfingenieur beim Einsatz eines Detektives durch seinen Arbeitgeber, der bei ihm eine Kfz-Hauptuntersuchung verdeckt als „normaler Kunde" durchführen lässt, keine Kenntnis darüber hat, dass er kontrolliert wird, ist bei der Beantwortung der Zulässigkeit einer solchen Vorgehensweise hier auch zwischen dem Rechtsgut der Verkehrssicherheit (Allgemeinwohl) und dem des Persönlichkeitsschutzes (Individualrecht) des Arbeitnehmers abzuwägen.

37 Vor dem Hintergrund, dass die behördliche Anerkennung der Prüforganisation von einer funktionsfähigen Innenrevision abhängt, die objektive Informationen über die Prüfwesen-Qualität, die festgestellte Mängelstruktur der überprüften Fahrzeuge sowie über die Plakettenkontrolle vorhalten muss, wird man eine solche Vorgehensweise als zulässig erachten müssen. Ein **milderes Mittel** würde hier nicht zur geforderten Objektivität führen, die der Einsatz eines Detektivs mit sich bringt.[30] Zu bedenken ist allerdings in einem solchen Fall, dass hier beim Mitarbeiter kein konkreter Verdacht auf

---

[27] Eine solche Auswertung ist mitbestimmungspflichtig. Das BAG 23.4.1985 – 1 ABR 39/81, DB 1985, 1897 f., hat dazu folgendes ausgeführt: „Der Antragsteller (TÜV) hat angeordnet, dass die Sachverständigen und Prüfer bei Ausfüllung der Prüfbelege ihre Personalkennziffer einzutragen haben. Die Prüfbelege werden in eine EDV-Anlage eingegeben und ausgewertet. Das Bundesarbeitsgericht hat auf Antrag des Gesamtbetriebsrats festgestellt, dass dem Gesamtbetriebsrat ein Mitbestimmungsrecht bei der maschinellen Auswertung der mit der Personalkennziffer versehenen Prüfbelege zusteht."

[28] *Wächter,* Datenschutz, Rn. 607.

[29] *Däubler,* Rn. 292 f.

[30] Insgesamt kritisch zu einer solchen verdeckten Ermittlung *Däubler,* Rn. 294; vgl. auch *Gola/Wronka,* Rn. 664 ff.

ein vertragswidriges Verhalten vorliegt, was eine Beauftragung eines Detektivs – nach § 11 iVm § 32 I 2 BDSG – grundsätzlich rechtfertigen würde.[31] Insofern lässt sich festhalten, dass es für eine **Routinekontrolle** durch Detektive – wie im dargelegten Fall der Überwachung der Prüftätigkeit – besonderer Gründe für die Zulässigkeit einer solchen Maßnahme bedarf. Auch präventive Maßnahmen unterliegen insofern prinzipiell einer Verhältnismäßigkeitsprüfung.

38 Fraglich ist, ob im Rahmen der Tätigkeit der Internen Revision auch das **Fotografieren des Prüfingenieurs** zulässig ist. Denn das allgemeine Persönlichkeitsrecht sichert zu, dass der Einzelne selbst darüber bestimmen kann, wie er sich in der Öffentlichkeit darstellt. Das Recht am eigenen Bild als Ausprägung des allgemeinen Persönlichkeitsrechts schützt vor einer **Verbreitung des Bildes,** sofern kein Rechtfertigungsgrund – zB eine Einwilligung oder §§ 23 f. KUG – vorliegt. Im Rahmen einer Routinekontrolle wird die Zulässigkeit der **Datenerhebung durch Fotografieren** zu verneinen sein. Dies ist nach § 32 I 1 BDSG auch nicht erforderlich. Es ist ausreichend, wenn der Detektiv an Hand des Prüfberichts des geprüften Fahrzeuges kontrollieren kann, ob der Prüfingenieur die vorhandenen Mängel festgestellt hat. Das Fotografieren der Mängel des Fahrzeugs ist natürlich erlaubt.

39 Grundsätzlich ist für die Interne Revision festzuhalten: Im Rahmen der Untersuchung – auch von Papierunterlagen – ist bei beschäftigtenbezogenen Daten „by name" eine Vorgehensweise festzulegen, welche die **Auswertungszwecke** und Untersuchungskriterien konkret beschreibt. Hier sollte jeweils geprüft werden, ob für die Auswertungszwecke auch anonymisierte bzw. pseudonymisierte Daten ausreichend sind. Denn hier stellt sich die Anwendbarkeit der Grenze der zulässigen Nutzung der Unterlagen nach § 32 I 1 und II BDSG, die dann gegeben wäre, wenn die erhobenen Daten für Zwecke der Durchführung oder Beendigung des Beschäftigungsverhältnisses verwendet werden.

2. Zulässige Formen der Datenerhebung und Compliance

a) Straftaten und IT-Compliance im Arbeitsverhältnis

40 Bei der Datenerhebung im Rahmen der Compliance ist zwischen der Verhinderung von **Pflichtverletzungen** und der Aufdeckung von **Straftaten** zu unterscheiden. Bei der Verhinderung von Pflichtverletzungen sowie der Etablierung darauf gerichteter Kontrollmaßnahmen geht es um präventive Kontrollmaßnahmen. Bei der Kontrolle der Einhaltung arbeitsvertraglicher Pflichten wie zB der Erfassung von Arbeitszeiten geht es um eine präventive Kontrollmaßnahme. Bei einer präventiven Maßnahme ist § 32 I 1 BDSG und bei der Aufdeckung von Straftaten § 32 I 2 BDSG anzuwenden.[32] Eine präventive Maßnahme ist danach prinzipiell eher zulässig als eine repressive Maßnahme.

41 Es wird in einem **normalen Beschäftigungsverhältnis** die Ausnahme darstellen, dass bei einem Arbeitnehmer nach § 32 I 2 BDSG tatsächliche Anhaltspunkte für einen Verdacht bestehen, dass er eine Straftat begangen hat. Damit besteht für den Arbeitgeber nach § 32 I 1 BDSG keine Legitimation, bei einem Arbeitnehmer Daten zur Verhinderung von Straftaten ohne konkreten Anlass zu erheben. Angesichts dessen ist die verdeckte und heimliche Form der Datenerhebung zur Erfassung mög-

[31] Dazu *Gola/Wronka,* Rn. 1177.
[32] *Gola/Schomerus,* § 32 Rn. 24.