# Compliance und Datenschutz

## Was Unternehmen bei Compliance-Maßnahmen beachten müssen

Korruptionsskandale bei Siemens, Datenlecks bei Rewe, Schmiergeldaffären bei Volkswagen und Lustreisen von Versicherungsvertretern von Ergo, aber auch die systematische Überwachung von Arbeitnehmern wie bei Lidl haben für viel Aufsehen in der Öffentlichkeit gesorgt. Diese können zu extremen Rufschädigungen führen und die Öffentlichkeitsarbeit der Marketingabteilung von Jahren zunichtemachen. Das Haftungsrisiko für die Geschäftsleitung einer Gesellschaft ist in den letzten Jahren unbestreitbar größer und die nationale und internationale Gesetzgebung durch die Globalisierung immer komplexer geworden. Neben den allgemeinen Haftungsrisiken droht selbst deutschen Unternehmen und deren Leitungen durch internationale (Antikorruptions-)Rechtsnormen wie den US Foreign Corrupt Practices Act (FCPA) und seit kurzem den UK Bribery Act des Vereinigten Königsreichs eine weitere verschärfte Haftung in Form von Bußgeldern-, und persönlicher Haftung.

### Corporate Compliance

Deutsche Unternehmen versuchen daher, aufkommenden Vorwürfen von Korruption, (Subventions-)Betrug, Schmiergeldzahlungen, Bestechung oder Untreue bereits im Vorfeld vorzubeugen. Um diesen Entwicklungen entgegenzuwirken, ist die Unternehmensleitung schon durch den Corporate Governance Kodex angehalten, eine Compliance-Organisation einzurichten. Der Begriff der Compliance stammt aus der anglo-amerikanischen Rechtssprache und bedeutet übersetzt „Entsprechung", „Einhaltung" oder „Befolgung". Übertragen auf den rechtlichen Bereich ist damit „Gesetzestreue" bzw. „dem Gesetz entsprechen" gemeint und das bedeutet sinngemäß, dass in Übereinstimmung mit geltenden Normen zu handeln ist.[1] Der Begriff der Compliance, seit längerem aus der Medizin bekannt,[2] und seine Funktionen haben ihren Ursprung im Bank- und Kapitalmarktrecht und in der Versicherungswirtschaft.[3] Zuletzt hat sich allerdings von der sog. „Wertpapier-Compliance"[4] ausgehend ein bereichs- und sektorübergreifendes Verständnis des Compliance-Begriffs durchgesetzt. Er beinhaltet eine Schutz-, Beratungs-, Informations-, Qualitätssicherungs-, Innovations-, Überwachungs- und Marketingfunktion.[5]

Allgemein ist unter Compliance ein Handeln in Übereinstimmung mit dem Gesetz oder – noch allgemeiner formuliert – mit den jeweils anwendbaren Regeln zu verstehen.[6] Für ein Unternehmen bedeutet dies heute die umfassende Einhaltung aller für seinen Geschäftsbereich maßgeblichen Gesetze und Normen sowie die Sicherstellung der Befolgung öffentlich-rechtlicher und strafrechtlicher Regeln. Compliance soll daher die Gesamtheit der Maßnahmen umfassen, die das rechtmäßige Verhalten eines Unternehmens, seiner Organe und Mitarbeiter im Hinblick auf alle gesetzlichen und unternehmenseigenen Gebote und Verbote gewährleisten.[7] Zur Herstellung von Compliance sind die Geschäftsführungsorgane von Unternehmen verpflichtet, für die sich ihre Pflicht aus der intern erforderlichen Sorgfalt oder gar aus internationalen Vorschriften wie dem Sarbanes-Oxley Act (SOX) ergibt.[8] Danach ist es die Aufgabe der Unternehmensleitung, für die Abwehr von Schäden, die Wahrung von Vorteilen[9] und die Pflicht zur Legalität zu sorgen.[10] Folglich ist es die Aufgabe insbesondere von Compliance-Officern, Organisationsabläufe durch Richtlinien, Trainings und Verhaltens- und Ethikkodizes innerhalb eines Unternehmens zu schaffen, deren Einhaltung zu überwachen und diesbezüglich Mitarbeiter zu schulen, damit die Regeln und Normen eingehalten werden. Auch wenn die Einhaltung der Gesetze für viele Anwender als „Binsenweisheit" oder „Selbstverständlichkeit" gilt, geht es letztlich bei Compliance nicht nur darum, „ob" die Gesetze und unternehmensinternen Richtlinien eingehalten werden, sondern „wie" sich dies bewerkstelligen lässt. Compliance umfasst daher sowohl Maßnahmen, die überwachen und aufdecken, ob die Legalitätspflicht der Unternehmensleitung eingehalten wird (präventives Merkmal), als auch solche, die darauf hinwirken, dass gesetzliche Pflichten gesellschaftsintern eingehalten werden (repressives Merkmal).[11] Letztere Maßnahmen sind u. a. die Geltendmachung von Unterlassungs- und Schadensersatzansprüchen, die Erklärung der außerordentlichen Kündigung oder die Einleitung strafrechtlicher Verfolgung.

### Spannungsfeld zwischen Compliance und Datenschutz

Bei der Durchsetzung von Compliance-Maßnahmen haben die Unternehmen allerdings auch die Rechte der Betroffenen, vorrangig die Grundsätze des Datenschutzes, zu wahren. So hat bereits das Bundesverfassungsgericht in seinem grundlegenden Urteil zur Volkszählung am 15.12.1983 festgestellt, dass es beim Datenschutz darum ginge, das Persönlichkeitsrecht der einzelnen betroffenen Person zu achten.[12] Als Ausfluss aus dem Grundrecht der informationellen Selbstbestimmung soll der Einzelne allein über die Preisgabe und die Verwendung seiner eigenen persönlichen Daten selbst entscheiden Dies gilt insbesondere dann, wenn es um die Umsetzung von Compliance-Maßnahmen im Unternehmen bei den Beschäftigten geht. Anders als im privaten Bereich kann der Betroffene

nicht in dem freien Ausmaß die Medien und Informationsquellen nutzen und sich der Überwachung entziehen. Er hat dabei aufgrund seiner ökonomisch bedingten Abhängigkeit die Anweisungen zu befolgen und Medien zu nutzen, die ihm der Arbeitgeber durch sein Direktionsrecht vorgibt. Somit ist zwischen den Interessen des Unternehmers und den besonderen Schutzbedürfnissen des Beschäftigten zu unterscheiden. Einerseits sind die Unternehmen zu Compliance-Maßnahmen wie der Korruptionsbekämpfung verpflichtet, andererseits ist dabei das Persönlichkeitsrecht des Arbeitnehmers zu beachten. So hat der Unternehmer bzw. Arbeitgeber die Pflicht, Schaden an seinem Eigentum zu verhindern und sicherzustellen, dass der Beschäftigte sein Eigentum nicht beschädigt, seine Dateneinrichtung nicht zu eigenen Zwecken missbraucht, und zu überwachen, dass der Beschäftigte seine Pflichten aus dem Arbeitsvertrag erfüllt.[13] Hingegen muss der Beschäftigte davor geschützt werden, ständig überwacht und kontrolliert zu werden, in seinem Handeln umfassend und ohne Anlass dokumentiert zu werden, zudem muss in seinem Persönlichkeitsrecht und seinem Wunsch nach Privatheit und seinem Grundrecht auf informationelle Selbstbestimmung respektiert werden.[14]

Jens Hertel © www.fotolia.de

Der Datenschutz will beachtet sein – auch bei Compliance-Maßnahmen.

### Datenschutz des Arbeitnehmers (Beschäftigtendatenschutz)

Bei allen Maßnahmen hat der Unternehmer die datenschutzrechtlichen Grenzen zu beachten, da es sich regelmäßig um sog. personenbezogene Daten i. S. d. § 3 Abs.1 BDSG handelt. Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten ergibt sich aus den Wertungen des BDSG. Danach besteht der Grundsatz, dass diese nur zulässig ist, soweit dieses Gesetz oder eine andere Rechtsvorschrift (z. B. Telemedien- oder Telekommunikationsgesetz) dies erlaubt oder der Betroffene einwilligt hat, vgl. § 4 BDSG. In den meisten Fällen ist daher eine Einwilligung i. S. d. § 4a BDSG erforderlich. Diese bedarf der Schriftform, wobei sie auch in elektronischer Form[15] erfolgen kann. Überdies muss der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung seiner Daten hingewiesen werden, sog. informierte Einwilligung.

Allerdings kommt der Einwilligung für die Verarbeitung von Beschäftigtendaten zur Erfüllung von Compliance-Pflichten nur eine nachrangige Bedeutung zu. In Beschäftigungsverhältnissen ergeben sich aufgrund der wirtschaftlichen Abhängigkeit des Beschäftigten vom Arbeitgeber hohe Anforderungen an die gemäß § 4a Abs. 1 BDSG erforderliche Freiwilligkeit der Einwilligung. Diese ist jedoch jederzeit widerrufbar und kann nicht dauerhaft einen einheitlichen Standard garantieren. Letztlich erscheint die Einholung der Einwilligung bei einem Verfahren mit einer großen Personengruppe als wenig praktikabel, da sie einen erheblichen organisatorischen Aufwand bedeutet.

1. Mitbestimmung
   Sofern ein Betriebsrat besteht, unterliegen Compliance-Maßnahmen regelmäßig der Mitbestimmung gemäß § 87 Abs. 1 Nr. 6 BetrVG. Die o. g. Probleme bei der Einwilligung lassen sich durch den Abschluss einer Betriebsvereinbarung vermeiden. In der Praxis werden daher regelmäßig Betriebsvereinbarungen über die Nutzung von Telekommunikationsmitteln geschlossen.
2. Einbeziehung des Datenschutzbeauftragten
   Bei Compliance-Maßnahmen ist es sinnvoll, den Datenschutzbeauftragten einzubeziehen. Er ist nicht nur darüber zu informieren gemäß § 4g Abs. 1, 2. Halbsatz, Abs. 2 S. 1 BDSG, sondern wird regelmäßig in diesen Fällen eine Vorabkontrolle nach § 4d Abs. 5 BDSG vornehmen müssen. Letztlich ist nicht zu unterschätzen, dass auch der Datenschutzbeauftragte aufgrund seiner Aufgabe auf die Einhaltung der Datenschutzgesetze hinzuwirken hat und damit Teil einer effektiven Compliance-Struktur ist. Erfährt er von Verletzungen von Persönlichkeitsrechten im Unternehmen, kann er sich unter Umständen strafbar machen.
3. Zulässigkeit der Maßnahmen:
   Die Zulässigkeit von Compliance-Maßnahmen richtet sich danach, ob es sich dabei um eine präventive oder repressive Maßnahme (s. o.) handelt. Maßgebend für die Prüfung der Zulässigkeit einer Compliance-Maßnahme ist es, ob eine präzise Dokumentation von deren Zweck und der vorgesehenen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorliegt. Bei der Erhebung personenbezogener Daten bedarf es eines konkreten Zwecks, für den die Daten verarbeitet oder genutzt werden. Diese Verarbeitung/Erhebung muss zudem „erforderlich" sein, d. h. allgemein dürfen im konkreten Fall keine anderen weniger belastenden und eingriffsintensiven Mittel geeignet sein, den Zweck zu erfüllen, wobei insoweit das Gebot der Datensparsamkeit aus § 3a BDSG zum

Tragen kommt. Verstoßen die Arbeitgeber bei ihren Maßnahmen gegen die Vorschriften des BDSG, kann dies gemäß § 43 mit einem Bußgeld von 300.000 Euro und höher als Ordnungswidrigkeit oder gar als Straftat gemäß § 44 bei vorsätzlichem Handeln geahndet werden.[16]

a) Präventive Maßnahmen

Die Überwachung bzw. Leistungs- und Verhaltenskontrolle der Beschäftigten der fällt grundsätzlich unter die Regelung des § 32 Abs. 1 S. 1 BDSG. Dies gilt etwa für Überprüfungen zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen, die im Zusammenhang mit der Durchführung des Beschäftigtenverhältnisses stehen. Einige Fälle davon sind:

- Überwachung der Einhaltung der internen Richtlinien (beispielsweise Verhaltenskodex),
- Datenabgleich („Screening") von Beschäftigtendaten in anonymisierter Form zur Korruptionsprävention oder
- Prüfung von Verstößen von Arbeitsverträgen, die jeweils personenbezogene Daten von Beschäftigten erheben, verarbeiten oder nutzen.

Mitarbeiter der Personalabteilung dürfen in bestehenden Beschäftigtenverhältnissen nur die Daten verarbeiten, die zur Durchführung des Beschäftigtenverhältnisses erforderlich sind. Dies sind meistens Daten, die für das zugrunde liegende Arbeitsverhältnis als geboten und nicht nur nützlich zu bewerten sind.[17] Alle anderen Daten, die nicht zum Beschäftigtenverhältnis zu zählen sind, fallen unter die unantastbare Privatsphäre des Beschäftigten (z. B. Hobbys, kulinarische Vorlieben etc.). Hingegen ist die Erhebung der Stammdaten als erforderlich in diesem Zusammenhang anzusehen, weil es sich um wichtige Grunddaten zur Person, wie Geschlecht, Alter, Adresse, Ausbildung und berufliche Qualifikationen handelt.

b) Repressive Maßnahmen

Bevor in Unternehmen Beschäftigtendaten zur Aufdeckung von bereits begangenen Straftaten verwendet werden dürfen, stellt § 32 Abs. 1 S. 2 BDSG vier Voraussetzungen auf, die kumulativ erfüllt sein müssen:

- tatsächliche Anhaltspunkte, die den Verdacht einer Straftat begründen,
- Dokumentation dieser Anhaltspunkte
- Erforderlichkeit der Erhebung, Verarbeitung und Nutzung der Beschäftigtendaten zur Aufklärung der Straftat und
- Abwägung der Interessen des Arbeitgebers an der Aufklärung gegen schutzwürdige Interesse der Beschäftigten unter Berücksichtigung von Art und Ausmaß im Hinblick auf den Anlass.

## Einzelne Beispiele aus der Praxis

a) Videoüberwachung (optisch-elektronische Einrichtung)

Die Videoüberwachung ist als klassisches Überwachungsinstrument für die Beobachtung öffentlich-zugänglicher Räume (z. B. Verkaufsräume im Kaufhaus, Schalterhalle im Bahnhof) in § 6b BDSG geregelt. Danach ist die Überwachung nur zulässig, wenn sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Auch hier ist im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen, ob die Zwecke im konkreten Fall nicht durch andere (mildere) Mittel erreicht werden können. Ist dies z. B. bei der Verhinderung von Diebstählen durch Taschenkontrollen, Inventuren oder Testkäufe möglich, so ist auf die Videoüberwachung zu verzichten.

Falls eine Videoüberwachung möglich ist, ist sie erkennbar (meistens durch ein Schild) zu machen. Bei der Ausrichtung der Überwachungskamera ist zudem u. a. von Bedeutung, wie viele Personen ihr ausgesetzt sind, ob diese anonym oder bekannt sind, ob sie einen Anlass für den Eingriff gegeben haben, insbesondere ob sie einer bereits begangenen oder drohenden Straftat oder Rechtsgutverletzung verdächtig sind, wo die Überwachungsmaßnahmen stattfinden, wie lange und intensiv sie sind und welche Technik dabei eingesetzt wird.[18] Eine permanente Kontrolle ist stets unzulässig, da sich Arbeitnehmer damit einem unzumutbaren Überwachungsdruck aussetzen würden. Maßgebend für die Zulässigkeit sind hierbei neben der Branche auch die konkreten Umstände des Einzelfalls. So sind für die Überwachung von Mitarbeitern in einem Restaurant andere Maßstäbe als bei einem Lagerraum eines Krankenhauses oder einem Tresorraum einer Bank anzusetzen, wobei bei einem Croupier im Spielcasino sogar eine durchgängige visuelle Überwachung möglich erscheint.[19]

In nicht-öffentlich zugänglichen Räumen (Büroräume, Werkshalle etc.) bestimmt sich die Zulässigkeit nach § 32 Abs. 1 S. 1 BDSG. Sie setzt voraus, dass die Erhebung von Beschäftigtendaten auch erforderlich ist. Dabei sind wegen der besonderen Intensität des Eingriffs in die Persönlichkeitsrechte hohe Anforderungen an das Merkmal der Erforderlichkeit zu stellen. So genügt nach allgemeiner Ansicht schon eine präventive Videoüberwachung ohne konkreten Grund nicht den Anforderungen des § 32 Abs. 1 S. 1 BDSG. Es müssen schon konkrete Anhaltspunkte wie eine erhöhte Anzahl von Diebstählen oder sonstige Straftaten gegen den Arbeitgeber sowie kein milderes Mittel zur Überwachung vorliegen.

Eine heimliche Überwachung ist allerdings nicht vom BDSG umfasst und auch nicht vom Gesetzgeber vorgesehen. Nach Rechtsprechung des BAG[20] ist diese grundsätzlich unzulässig. Eine Ausnahme besteht allerdings in den (repressiven) Fällen, in denen ein Mitarbeiter des Diebstahls verdächtigt wird. Hier darf der Arbeitgeber mit Zustimmung des Betriebsrats versuchen, ihn per Videoüberwachung zu überführen. Hier gelten die strengen Voraussetzungen des § 32 Abs. 1 S. 2 BDSG.

Ausgenommen von jeder Überwachung sind Betriebsstätten, die überwiegend der privaten Lebensgestaltung des Beschäftigten dienen (Umkleide-, Schlaf- und Ruheräume sowie Sanitärräume). Eine

Krankenschwester darf daher im Bereitschaftszimmer nicht überwacht werden, weil dieses zum Ausruhen dient.

b) Überwachung von Multimedia am Arbeitsplatz

Über die Kontrolle der E-Mail-, Telefon- und Internetnutzung wurde viel diskutiert. Die Zulässigkeit hängt nicht nur vom Einzelfall und Unternehmensbranche, sondern auch von der Eingriffsintensität in das Persönlichkeitsrecht ab. Unternehmen, die übers Telefon oder Internet Geschäfte abschließen, z. B. der Verkauf von Gas, dürfen Gespräche und Korrespondenzen der Beschäftigten nicht nur umfassender überwachen als gewöhnliche Dienstleitungsunternehmen, sondern auch automatisch aufzeichnen.[21] Vielmehr kommt es bei der Überwachung darauf an, ob der Arbeitgeber alle Daten über Telefonate wie Uhrzeit, Zielnummer bzw. E-Mail- und Internetdaten seiner Beschäftigten speichern und verwenden darf. Das Recht zur Überwachung richtet sich in erster Linie danach, ob die Kommunikationsmittel durch den Arbeitnehmer auch privat genutzt werden dürfen. Ist eine Nutzung zu privaten Zwecken verboten, darf der Arbeitgeber die Daten grundsätzlich speichern. Sofern jedoch eine private Nutzung erlaubt ist, sind seine Kontrollrechte stark eingeschränkt, denn nach allgemeiner Ansicht wird er damit zum Diensteanbieter i. S. d. des TKG und muss das Fernmeldegeheimnis beachten. Leistungs- und Verhaltenskontrollen sind daher verboten, wenn sich die private und die dienstliche Nutzung nicht eindeutig (z. B. durch Zugangscodes) trennen lassen. Allerdings bleibt der Arbeitgeber – auch bei geduldeter Privatnutzung – befugt, Angaben über Telefongespräche, etwa im Rahmen einer stichprobenartigen Kosten- und Wirtschaftlichkeitskontrolle, zu verarbeiten. Dies kann z. B. bei einer exzessiven privaten Nutzung durch den Beschäftigten erfolgen. Dabei sind Daten, die eine Identifizierung des Angerufenen erlauben, ihm unzugänglich zu machen. Dasselbe gilt für die Angabe der eingehenden Privatgespräche. In der Praxis haben viele Unternehmen wegen der vielen individuellen Gegebenheiten eine Nutzung von Multimedia in Betriebsvereinbarungen näher geregelt.

c) Ortungssysteme
(GPS oder Handy-Ortung)

Eine Überwachung von externen bzw. mobil tätigen Beschäftigten ist auch durch den Einsatz von Ortungssystemen möglich. In diesem Zusammenhang können regelrechte Bewegungs- und Verhaltensprofile z. B. von Fahrern einer Spedition angefertigt werden. Der Einsatz von Ortungssystemen ist folglich nicht unbegrenzt möglich. Während der Arbeits- und Betriebszeit dürfen Daten unter bestimmten Voraussetzungen erhoben werden, wenn sie der Sicherheit des Beschäftigten, von sehr wertvollen zu transportierenden Gegenständen oder dazu dienen, den Einsatz zu koordinieren. Dies betrifft beispielsweise Speditionen, bei denen eine Ortung erforderlich i. S. d. des § 32 Abs. 1 S.1 BDSG ist. Eine heimliche Ortung, wie der verdeckten Anbringung eines GPS-Senders von Beschäftigten ist verboten, und kann eine Straftat nach §§ 44 Abs. 1, 43 Abs. 2 Nr. 1 BDSG darstellen.[22]

Dieselben Maßstäbe gelten bei der Ortung von Handys, allerdings muss hierbei beachtet werden, dass der Arbeitgeber als Teilnehmer gegenüber dem Anbieter des Telekommunikationsdienstes seine Einwilligung erklären und seinen Beschäftigten gemäß § 98 TKG davon zu unterrichten hat.

**Hinweis:**

**Im Frühjahr 2009 wurde bekannt, dass der Lebensmitteldiscounter Lidl die Krankheiten von Mitarbeitern systematisch festgehalten hat. Bereits ein Jahr zuvor hatte das Unternehmen für Schlagzeilen gesorgt, weil es Mitarbeiter mit versteckten Kameras überwacht hatte. Auch Kunden wurden dabei gefilmt. Protokolle vermerkten etwa, wann eine Mitarbeiterin auf die Toilette ging oder Pause machte.**

1 Vgl. unter vielen: Mengel/Hagemeister, BB 2006, 2466, 2466.
2 So nachzulesen in Hauschka, NJW 2004, 257, 257 unter Hinweis auf: OLG Hamburg, GRUR-RR 2003, 105.
3 Nave, BB 2008, 734, 734.
4 Siehe dazu Hense/Renz, CCZ 2008, 181, 181 f.
5 Lösler, NZG 2005, 104, 104 m. w. N.
6 Vgl. Schneider, ZIP 2004, 645, 646.
7 Thüsing, Arbeitnehmerdatenschutz und Compliance, 2010, S. 9, Rdnr. 9.
8 Diese folgt aus § 93 AktG oder § 30 OWiG
9 BGHZ 21, 354, 357, Fleischer, in: Spindler/Stilz, AktG, § 93, Rn. 11.
10 Reichert/Ott, ZIP 2009, S. 2173.
11 Thüsing, Arbeitnehmerdatenschutz und Compliance, 2010, S. 9, Rdnr. 9.
12 Bundesverfassungsgericht vom 15.12.1983, – 1 BvR 209, 269, 362, 420, 440, 484/83 – BVerfGE 65,1 ff. = NJW 1984, 419
13 Joussen, NZA-Beilage 2011, S. 35, 37.
14 Thüsing, Arbeitnehmerdatenschutz und Compliance, 2010, S. 1, Rdnr. 2.
15 Insoweit gelten die Anforderungen des § 13 Abs. 2 und 3.
16 zuletzt Landgericht Lüneburg, Beschluss vom 28.03.2011, 26 Qs4 45/11.
17 Däubler, NZA 2001, 874, 877.
18 Bundesarbeitsgericht, Beschluss vom 29.06.2004 – 1 ABR 21/03 – NZA 2004, 1278, 1278.
19 Vgl. Landesarbeitsgericht Berlin-Brandenburg, Beschluss vom 09.09.2011, Az. 6 TaBV 851/11.
20 Bundesarbeitsgericht, Beschluss vom 29.06.2004 – 1 ABR 21/03 – NZA 2004, 1278 ff.
21 Siehe zur Aufzeichnung bei Gasversorgungsunternehmen, Starke, RDV 2011, 177 ff.
22 Landgericht Lüneburg, Beschluss vom 28.03.2011, 26 Qs4 45/11.

PATRICK KNITTEL
Doktorand
Dozent für Recht und Datenschutz
juristischer Referent bei Alpmann Schmidt
Berlin