Handlungsempfehlungen im Überblick

Der neue Beschäftigtendatenschutz

Hanno Timner
ist Rechtsanwalt und Partner im Berliner Büro der internationalen Sozietät Hogan Lovells.

Dr. Michael Schreier
ist Rechtsanwalt und Associate im Hamburger Büro von Hogan Lovells.

Die Nutzung von Beschäftigtendaten wirft in der Praxis zahlreiche Fragen auf, die bislang nicht oder nur unbefriedigend gelöst sind. Der Gesetzgeber hat die in diesem Bereich bestehenden Rechtsunsicherheiten über viele Jahre hinweg in Kauf genommen. Dies soll sich nun ändern.

1 Offene Fragen und Datenschutzskandale

Darf ein Arbeitgeber auf die E-Mails seiner Mitarbeiter zugreifen, wenn diese krank oder im Urlaub sind? Welche Kontrollrechte stehen ihm zu, wenn er einen Arbeitnehmer verdächtigt, während der Arbeitszeit exzessiv im Internet zu surfen und „verbotene Inhalte" aufzurufen? Blockiert die einmal erlaubte private Internetnutzung hier jegliche Überprüfung oder genügt es, wenn sich der Arbeitgeber die schriftliche Einwilligung für Kontrollmaßnahmen von seinen Beschäftigten erteilen lässt? Die Liste offener und in der Praxis umstrittener Fragen lässt sich beliebig fortsetzen.

Die im vergangenen Jahr bekannt gewordenen „Datenschutzskandale" in mehreren deutschen Unternehmen haben als Weckruf gedient und den Gesetzgeber zum Handeln veranlasst. Der jetzt vorliegende Gesetzentwurf zum Beschäftigtendatenschutz vom 25.8.2010 nimmt hierbei teils die bereits in der Rechtsprechung und von den Datenschutzbehörden vertretenen Rechtspositionen auf und regelt erstmals ausdrücklich auch so praxisrelevante Bereiche, wie die Nutzung von E-Mail und Internet durch Arbeitnehmer und deren Kontrolle durch Arbeitgeber.

2 Status quo – die derzeitige Rechtslage

Seit dem 1.9.2009 findet sich mit § 32 Bundesdatenschutzgesetz (BDSG) erstmals eine ausdrückliche gesetzliche Regelung zum Datenschutz im Beschäftigtenverhältnis. Zuvor galten die allgemeinen Vorschriften des BDSG und die – ausgesprochen spärlichen – von der Rechtsprechung und den Datenschutzbehörden entwickelten Grundsätze, z. B. zur Videoüberwachung oder zur Kontrolle von Internet- und E-Mail-Nutzung. § 32 BDSG ist derzeit die zentrale Norm zum Beschäftigtendatenschutz. Er gilt nicht nur für Mitarbeiter, sondern auch für Bewerber um ein Beschäftigungsverhältnis. Grundaussage des § 32 BDSG ist, dass Arbeitgeber Arbeitnehmerdaten nur erheben, verarbeiten und nutzen dürfen, wenn dies für die

- Einstellungsentscheidung,
- Durchführung oder
- Beendigung

eines Beschäftigungsverhältnisses „erforderlich" ist.

Besondere Regeln gelten für Maßnahmen zur Aufdeckung von Straftaten: Zu diesem Zweck darf der Arbeitgeber Beschäftigtendaten erheben oder verwenden, wenn

- tatsächliche Anhaltspunkte einen Verdacht gegen einen Mitarbeiter begründen und
- er diese Anhaltspunkte dokumentiert hat.

Neben der Verarbeitung personenbezogener Daten im Arbeitsverhältnis gem. § 32 BDSG kommt in Einzelfällen auch eine Nutzung dieser Daten nach der im nicht-öffentlichen Bereich maßgeblichen „Generalklausel" des § 28 BDSG infrage.

3 Regelungsbedarf

Insgesamt lässt der aktuelle § 32 BDSG viele Fragen offen. So ist etwa unklar, welcher Maßstab im Hinblick auf die „Erforderlichkeit" der Datenerhebung anzulegen ist. Bei einer strengen Auslegung wäre hier schon zweifelhaft, ob der Arbeitgeber etwa die Kontendaten der Arbeitnehmer erfassen darf, könnte er doch – zugegeben eher theoretischerweise – das Gehalt auch am Ende des Monats bar auszahlen. Ebenso umstritten ist, ob er personenbezogene Daten seiner Mitarbeiter unter den gleichen Voraussetzungen für die Aufklärung von Ordnungswidrigkeiten und schwer wiegenden Vertragsverstößen erheben und nutzen darf, wie sie für die Aufklärung von Straftaten gelten („tatsächliche, zu dokumentierende Anhaltspunkte einer Straftat des Beschäftigten").

Auch die in der Praxis bei den meisten Arbeitgebern nahezu täglich vorkommende Frage, ob sie die Internet- oder E-Mail-Nutzung ihrer Arbeitnehmer kontrollieren dürfen, ist bisher nicht ausdrücklich im Gesetz geregelt. Da diese Sachverhalte zudem nur in seltenen Ausnahmefällen die Gerichte beschäftigt haben, bietet auch die Rechtsprechung in der Praxis keine verlässliche Entscheidungsgrundlage. Schließlich vertreten selbst die Datenschutzbehörden der Länder z. T. deutlich unterschiedliche Rechtsstandpunkte zu identischen Sachverhalten.

Wichtig

In der Praxis führt dies dazu, dass Arbeitgeber bei der Nutzung personenbezogener Daten ihrer Mitarbeiter einer erheblichen Rechtsunsicherheit ausgesetzt sind und Gefahr laufen, einen – ggf. bußgeldbewehrten – Verstoß gegen die Regelungen des BDSG zu begehen.

4 Anwendungsbereich der geplanten Neuregelungen

Am 25.8.2010 hat die Bundesregierung einen zum wiederholten Male überarbeiteten Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes als Regierungsentwurf (BDSG-E) vorgestellt. Dieser sieht insgesamt zwölf neue Paragrafen vor, die in einem eigenen Kapitel neben § 32 als §§ 32a bis 32l das BDSG ergänzen sollen. Die §§ 32a und 32b BDSG-E regeln dabei, wie Unternehmen Mitarbeiterdaten vor Begründung des Beschäftigungsverhältnisses verwenden dürfen. Die §§ 32c ff. BDSG-E beziehen sich auf die Datenverarbeitung während des Arbeitsverhältnisses.

Übersicht

Anwendungsbereich §§ 32 bis 32l BDSG-E

Persönlicher Anwendungsbereich

Unter den persönlichen Anwendungsbereich der neuen Regelungen zum Beschäftigtendatenschutz fallen
- Bewerber für ein Beschäftigungsverhältnis,
- gegenwärtige und ehemalige Arbeitnehmer und
- Auszubildende.

Sachlicher Anwendungsbereich

In sachlicher Hinsicht erfassen die geplanten Vorschriften sowohl die automatische Datenverarbeitung, z. B.
- bei der Zeiterfassung oder
- in der Lohnbuchhaltung,

als auch die nicht automatische Datenverarbeitung, wie
- den Blick in die Personalakte,
- Fragen im Bewerbungsgespräch oder
- handschriftliche Aufzeichnungen.

5 Ende der Generalklausel

Nach der Begründung des Gesetzentwurfs soll sich die Verwendung von Mitarbeiterdaten vor, nach und im Beschäftigungsverhältnis zukünftig ausschließlich nach den neuen Vorschriften richten. Insbesondere gilt die bisherige „Generalklausel" des § 28 BDSG für Arbeitnehmerdaten zukünftig nicht mehr. Sie kommt nur noch zur Anwendung, sofern der Arbeitgeber Arbeitnehmerdaten neben dem eigentlichen Beschäftigungsverhältnis erhebt.

Beispiele

Ein Bankmitarbeiter eröffnet ein Bankkonto, der Mitarbeiter einer Versicherung schließt mit dem Arbeitgeber Versicherungsverträge ab oder der Beschäftigte eines Autoherstellers kauft ein Fahrzeug.

Der Bundesrat hat in seiner Sitzung vom 5.11.2010 dazu beschlossen, es sei festzulegen, dass Arbeitgeber personenbezogene Daten, die sie aus anderen mit ihren Arbeitnehmern geschlossenen Verträgen erheben, nicht für Zwecke des Arbeitsverhältnisses verarbeiten und nutzen dürfen. Es bleibt abzuwarten, ob sich der Bundesrat im Gesetzgebungsverfahren damit durchsetzen kann.

Kern der vorgeschlagenen Neuregelungen ist – wie bereits beim bisherigen § 32 BDSG –, dass es vor, nach oder im laufenden Beschäftigungsverhältnis für dessen Zwecke „erforderlich" sein muss, die Daten zu erheben oder zu nutzen.
Darüber hinaus sieht der Gesetzentwurf ausdrückliche Regelungen für besondere Sachverhalte vor. So finden sich u. a. Vorschriften hinsichtlich

- Korruptionsbekämpfung und Compliance (§§ 32d Abs. 3, 32e BDSG-E),
- Videoüberwachung (§ 32f BDSG-E),
- Einsatz von Ortungssystemen (§ 32g BDSG-E),
- Einsatz biometrischer Verfahren (§ 32h BDSG-E) sowie
- Nutzung von Telekommunikationsdiensten (§ 32i BDSG-E).

Wichtig

Bislang haben Unternehmen in vielen Fällen die Einwilligung der betroffenen Beschäftigten in eine Datenerhebung oder -verwendung eingeholt, um diese zu legitimieren, z. B. bei einer verlängerten Speicherfrist der Bewerberdaten. Für die Praxis von erheblicher Bedeutung ist nun, dass nach § 32l BDSG-E dieses Vorgehen nur noch in wenigen, ausdrücklich geregelten Ausnahmefällen zulässig ist, so dass Arbeitgeber die Nutzung personenbezogener Daten ihrer Arbeitnehmer zukünftig regelmäßig nicht mehr auf deren Einwilligung stützen können, sondern darauf angewiesen sind, dass ein ausdrücklicher gesetzlicher Erlaubnistatbestand vorliegt.

Es ist auch zukünftig unerlässlich, die Vorschriften zum Beschäftigtendatenschutz einzuhalten. Schon nach der derzeitigen Rechtslage können Rechtsverstöße mit Bußgeldern i. H. v. bis zu 300.000 Euro geahndet werden. Liegt zusätzlich eine Bereicherungs- oder Schädigungsabsicht vor, droht als Straftatbestand sogar eine Freiheitsstrafe von bis zu zwei Jahren. Dies ändert sich auch nach dem Gesetzentwurf nicht, §§ 43, 44 BDSG-E.

6 Fragerecht des Arbeitgebers im Bewerbungsverfahren

Für die Praxis hilfreiche Klarstellungen enthält der Gesetzentwurf zunächst im Hinblick auf das Fragerecht des Arbeitgebers im Bewerbungsverfahren (§ 32 Abs. 2 BDSG-E), vgl. im Detail dazu Hunold, S. 17 ff. in diesem Heft.
Er darf danach nur diejenigen Informationen erforschen, die für das konkret vorgesehene Arbeitsverhältnis von Bedeutung sind. Daten eines Beschäftigten zur rassischen und ethnischen Herkunft, Religion oder Weltanschauung, Behinderung, sexuellen Identität, Gesundheit sowie zu Vermögensverhältnissen, Vorstrafen oder laufenden Ermittlungsverfahren darf er dagegen nur unter den Voraussetzungen des § 8 Abs. 1 AGG erheben, d. h. wenn entsprechende Merkmale ausnahmsweise für die Eignung des Bewerbers eine entscheidende Rolle spielen. Auch Fragen nach einer Schwangerschaft, dem Kinderwunsch einer Arbeitnehmerin oder Vorstrafen sind im Regelfall unzulässig, falls sie nicht ausnahmsweise Rückschlüsse darauf zulassen, ob der Bewerber für die konkrete Stelle geeignet ist.

Beispiel

Der Arbeitgeber darf etwa den zukünftigen Buchhalter danach fragen, ob er bereits Vermögensdelikte begangen hat, oder den Kraftfahrer, ob er wegen Trunkenheitsfahrten vorbestraft ist. Entsprechende Fragen an die Bewerberin für eine Sekretariatsstelle wären dagegen eindeutig unzulässig.

Wichtig

Informationen über Bewerber sind grundsätzlich bei diesen direkt zu erheben. Will der Arbeitgeber eigene Nachforschungen anstellen, muss er vorab hierauf hinweisen, etwa in der Stellenausschreibung. Ein Zugriff auf soziale Netzwerke, wie Facebook & Co., die – anders als bspw. Xing – nicht der beruflichen Vernetzung dienen, ist unzulässig, § 32 Abs. 6 BDSG-E, vgl. auch Schmid/Appt, S. 23 ff. in diesem Heft.

Dem gleichen Muster folgen die Regeln zu ärztlichen Gesundheitsprüfungen. Auch hier kann der Arbeitgeber eine Untersuchung nur verlangen, wenn das Ergebnis maßgeblich dafür ist, ob sich der Bewerber für die konkrete Stelle eignet, und er der Untersuchung ausdrücklich zugestimmt hat. Bei Blutuntersuchungen ist der Bewerber über den genauen Umfang der geplanten Tests aufzuklären und muss diesen zustimmen, vgl. Raif, S. 34 ff. in diesem Heft.

Beispiel

Die an einen Chirurgen gerichtete Bitte um eine HIV- oder Hepatitis-C-Untersuchung ist zulässig, allgemeine Blutuntersuchungen auf Alkohol- oder Drogenmissbrauch bei sonstigen Beschäftigten dagegen nicht.

7 Videoüberwachung

Die Videoüberwachung in nicht öffentlich zugänglichen Betriebsstätten war bislang gesetzlich nicht geregelt. Lediglich für öffentlich zugängliche Räume, z. B. Verkaufsflächen in Einzelhandelsgeschäften, Kinos etc., galt und gilt weiterhin die Sonderregelung des § 6b BDSG, wonach die Videoüberwachung grundsätzlich „zur Wahrung berechtigter Interessen" erforderlich sein muss. Im Übrigen finden nach aktueller Rechtslage die von der Rechtsprechung entwickelten Grundsätze Anwendung, vgl. zum Thema auch Lang, S. 26 ff. in diesem Heft:

- Eine verdeckte Videoüberwachung am Arbeitsplatz ist nur kurzfristig und gewissermaßen als „letztes Mittel" bei konkretem Verdacht von Straftaten zulässig, wenn weniger einschneidende Maßnahmen nicht zur Verfügung stehen.
- Die offene Videoüberwachung ist lediglich erlaubt, soweit sie erforderlich ist, um wichtige betriebliche Interessen zu wahren und sie außerdem verhältnismäßig ist. Dies kann bspw. im Eingangsbereich eines Unternehmens der Fall sein. Sie unterliegt aber der Einschränkung, dass der Arbeitgeber die mildeste Form der Durchführung wählen muss, z. B. die Überwachung auf einzelne, besonders gefährdete Betriebsteile beschränken oder sie bloß am Bildschirm durchzuführen, statt die Bilder aufzuzeichnen.

Die im Gesetzentwurf vorgesehene Neuregelung in § 32f BDSG-E bezieht sich auf eine offene Videoüberwachung in nicht öffentlich zugänglichen Räumen:

- Eine offene Videoüberwachung soll zulässig sein, soweit sie erforderlich ist, um wichtige betriebliche Interessen zu wahren. Die Vorschrift nennt ausdrücklich u. a. die Wahrnehmung des Hausrechts, den Schutz des Eigentums und die Sicherheit der Beschäftigten. Ferner hat eine Abwägung mit den Interessen der Beschäftigten zu erfolgen. Arbeitgeber, die eine offene Videoüberwachung durchführen wollen, müssen dies durch geeignete Maßnahmen, etwa Hinweisschilder, erkennbar machen.

Wichtig

Der Gesetzentwurf legt auch fest, dass der Arbeitgeber Bereiche, die überwiegend zur privaten Lebensgestaltung der Beschäftigten bestimmt sind, nicht überwachen darf. Insbesondere ist eine Videoüberwachung in Sanitär-, Umkleide- und Schlafräumen unzulässig.

- Eine verdeckte Videoüberwachung ist nach derzeitigem Stand des Gesetzentwurfs überhaupt nicht zulässig. Vorherige Entwürfe haben sie unter bestimmten Voraussetzungen hingegen noch als zulässig festgelegt. Es bleibt abzuwarten, ob es im Laufe des Gesetzgebungsverfahrens noch Änderungen in diesem Punkt geben wird.

8 Problem: Kontrollrechte bei Telekommunikation

Das in der Praxis wohl wichtigste datenschutzrechtliche Thema ist sicherlich, ob und in welchem Maße Arbeitgeber die (private) Nutzung moderner Kommunikationsmittel, wie Telefon, Internet und E-Mail, durch ihre Arbeitnehmer kontrollieren dürfen, s. dazu auch Keilich, S. 30 ff. in diesem Heft. Nach der bisherigen Rechtslage kommt es bei der Frage, ob es dem Arbeitgeber gestattet ist, Verbindungsdaten, z. B. angerufene Telefonnummer, Tag, Uhrzeit sowie Beginn und Ende eines Gesprächs, und Inhalte der Telefon-, Internet- und E-Mail-Kommunikation zu ermitteln und auszuwerten, vor allem darauf an, ob er die Privatnutzung erlaubt hat bzw. sie zumindest duldet.

Im Fall der erlaubten oder – in der Praxis häufig anzutreffenden – geduldeten Privatnutzung sind den Möglichkeiten, die Telekommunikationsnutzung zu überwachen, enge Grenzen gesetzt. Der Arbeitgeber gilt als Anbieter einer Telekommunikationsdienstleistung. Er unterliegt daher den Vorschriften des Telekommunikationsgesetzes (TKG), insbesondere dem Fernmeldegeheimnis des § 88 TKG. Die gegenwärtig noch herrschende Meinung geht deshalb davon aus, dass der Arbeitgeber Inhalte und Verbindungsdaten nur in engen Grenzen erheben und verwenden darf, bspw. zu Abrechnungszwecken, um die technischen Systeme zu schützen oder zu warten. Eine Erhebung oder Verwendung zu anderen Zwecken sei verboten und soll unter Strafe stehen. Daran ändere auch der Umstand nichts, dass der Arbeitgeber ein grundsätzliches Zugriffsrecht auf die Arbeitsergebnisse seiner Arbeitnehmer hat.

Praxistipp

Eine geduldete Privatnutzung kann auch vorliegen, wenn der Arbeitgeber, obwohl er die private Nutzung untersagt hat, das Verbot in der Praxis nicht konsequent „lebt", d. h. Verstöße „sehenden Auges" akzeptiert. In der Praxis sollte man daher darauf achten, dass die Mitarbeiter das Verbot auch einhalten.

9 Bisherige Rechtsprechung zur E-Mail-Überwachung

Bislang hat sich die Rechtsprechung nur vereinzelt mit der Reichweite des Fernmeldegeheimnisses beschäftigt. Nach einer Entscheidung des BVerfG aus dem Jahr 2006 reicht der Grundrechtsschutz des Fernmeldegeheimnisses bei E-Mail-Verkehr nur bis zu dem Zeitpunkt, in dem die E-Mail beim Empfänger ankommt und der Übertragungsvorgang abgeschlossen ist (Urt. v. 2.3.2006 – 2 BvR 2099/04). Unter Berücksichtigung dessen hat z. B. der Verwaltungsgerichtshof (VGH) Kassel am 19.5.2009 entschieden (6 A 2672/08.Z, AuA 7/10, S. 440 f.), dass das TKG den Arbeitgeber nicht daran hindert, die auf einem auch privat genutzten Computer gespeicherten E-Mail-Ordner einzusehen.

Die Entscheidung des BVerfG betraf jedoch keinen arbeitsrechtlichen Sachverhalt und das Urteil des VGH Kassel steht bislang allein auf weiter Flur. Die vorherrschende Ansicht ist daher noch immer, dass Arbeitgeber,

die eine private Nutzung erlauben oder tolerieren, aufgrund des Fernmeldegeheimnisses an der Kontrolle von E-Mail-Korrespondenz ihrer Mitarbeiter grundsätzlich auch nach Eingang der E-Mails beim Arbeitnehmer gehindert sind. Diese Kontrollsperre erstreckt sich nicht nur auf die privaten, sondern auch auf die hierdurch „infizierten" dienstlichen E-Mails. Gegenläufige Stellungnahmen der zuständigen Datenschutzbehörden existieren nicht. Die – zutreffende – Sicht des BVerfG und des VGH Kassel zu den Grenzen des Fernmeldegeheimnisses und damit zur Zulässigkeit von Arbeitgeberkontrollen hat sich bisher nicht durchgesetzt.

10 Regelungen zur Telekommunikationsnutzung

Diese für Arbeitgeber ausgesprochen unbefriedigende Rechtslage soll sich nach dem gegenwärtigen Stand des Gesetzentwurfs ändern. Er stellt nun die Kontrolle der Telekommunikationsnutzung der Mitarbeiter durch Arbeitgeber klar. Zukünftig gelten folgende Grundsätze:

- Der Arbeitgeber darf Verkehrsdaten der Telekommunikation (angewählte Telefonnummer, aufgerufene Internetseite, Datum, Uhrzeit und Dauer der Telekommunikation) bei rein dienstlicher Nutzung aus technischen Gründen, zu Abrechnungszwecken oder für stichprobenartige Leistungs- und Verhaltenskontrollen überprüfen, § 32i Abs. 1 BDSG-E. Erhebt er diese Daten, um die Leistung und das Verhalten zu kontrollieren, muss er den betroffenen Arbeitnehmer nachträglich hierüber informieren.
- Die erlaubte private Telekommunikationsnutzung der Mitarbeiter und die hieraus etwa folgenden Einschränkungen bei der Kontrolle durch den Arbeitgeber regelt der Gesetzentwurf nicht. Die Gesetzesbegründung stellt aber klar, dass das Fernmeldegeheimnis auch hier jedenfalls für Telekommunikationsvorgänge gilt, die noch andauern, also z. B. ein laufendes Telefongespräch oder das Aufrufen einer Internetseite.
- Nach Abschluss des Telekommunikationsvorgangs, z. B. wenn die E-Mails im Account eingegangen sind, ist der Arbeitgeber – unabhängig von einer etwa gestatteten privaten Nutzung – befugt, dienstliche E-Mails nach allgemeinen datenschutzrechtlichen Grundsätzen (§§ 32c, 32d BDSG-E) einzusehen, zu nutzen und zu kontrollieren. Er darf also ohne Erlaubnis des Arbeitnehmers dessen E-Mails nutzen, wenn der Betreffende krankheitsbedingt abwesend oder während einer laufenden Kündigungsfrist freigestellt ist.
- Private E-Mails darf der Arbeitgeber nach Eingang im E-Mail-Account einsehen, wenn dies für den ordnungsgemäßen Geschäftsbetrieb unerlässlich ist, etwa wenn er während der Erkrankung des Arbeitnehmers dessen dienstliche E-Mails verarbeiten muss und hierbei auch auf private E-Mails stößt. Weitere Voraussetzung ist, dass er den Beschäftigten auf diese Möglichkeit zuvor schriftlich hingewiesen hat.

Wichtig

Besondere Vorsicht ist aber weiterhin bei der Kontrolle von noch andauernden Telefongesprächen der Mitarbeiter geboten. Hier gilt nach bisheriger – wie auch zukünftiger – Rechtslage, dass es grundsätzlich unzulässig und strafbewehrt ist, Telefongespräche heimlich mitzuhören oder aufzuzeichnen. Nur wenn der Beschäftigte und sein Kommunikationspartner im Einzelfall über das Mithören informiert wurden und ausdrücklich vorher eingewilligt haben, ist dies zulässig. Der Arbeitgeber muss zudem ein berechtigtes Interesse am Mithören nachweisen können.

Eine Ausnahme besteht nach dem Gesetzentwurf (§ 32i Abs. 2 BDSG-E) aber, wenn die Nutzung von Telefondiensten zum wesentlichen Inhalt der geschuldeten Arbeitsleistung gehört, z. B. bei Callcenter-Mitarbeitern. Dann darf der Arbeitgeber Telefongespräche stichprobenartig auch ohne konkrete Kenntnis des Beschäftigten im Einzelfall mithören, allerdings nur, wenn

- er sowohl den Arbeitnehmer als auch seinen Kommunikationspartner grundsätzlich über die Möglichkeit einer solchen Kontrolle informiert,
- der Kommunikationspartner einwilligt, wobei die vorbehaltlose Fortsetzung des Telefonats als Einwilligung gilt, und
- er den Mitarbeiter anschließend benachrichtigt, dass das Telefongespräch mitgehört wurde.

11 Fazit

Die geplanten Änderungen im Beschäftigtendatenschutzgesetz werden die Rechtslage erheblich ändern. Zahlreiche Neuerungen stehen auf der Tagesordnung. Dies gilt insbesondere in Bezug auf die Kontrolle der Telekommunikation im Betrieb.