

6. dtb-Forum für Arbeitnehmervertreter 2011

Compliance, Arbeitnehmerdatenschutz und neuer § 32 BDSG

Manfred Ilgenfritz
Bayerisches Landesamt für Datenschutzaufsicht

Einzelthemen:

- Datenschutzkonformes Arbeitnehmerscreening
- Instrument Whistle-Blowing
- Grenzen von Ermittlungen
- Meldepflicht bei Datenpannen gem. § 42a BDSG

Einführung:

Compliance bedeutet "**Regeltreue**", hier also die Einhaltung von allen relevanten Gesetzen und betrieblichen Richtlinien durch alle für ein Unternehmen tätigen Personen, angefangen vom Vorstand oder Geschäftsführer bis zu den Beschäftigten in der Produktion und den Auszubildenden.

Regelverstöße kommen bekanntermaßen auf allen Hierarchieebenen vor, von Betrugs-, Untreue- und Korruptionsfällen im Führungsbereich bis zur widerrechtlichen Verwendung oder Unterschlagung betrieblicher Mittel für private Zwecke durch Hilfskräfte.

Weil bestimmte gewichtige Regelverstöße den Erfolg eines Unternehmens relevant beeinträchtigen und den Betriebsfrieden erheblich stören können, haben grundsätzlich alle Akteure in einem Unternehmen - Eigentümer, Führung und Mitarbeiter - ein Interesse an der Verhinderung bzw. zumindest Eingrenzung solcher Verstöße.

Manche Gesetze enthalten auch Verpflichtungen für Unternehmen, angemessene Compliance-Maßnahmen zum Schutz des Unternehmens durchzuführen, wie das Aktiengesetz oder das Kreditwesengesetz.

Aktuelles Praxisbeispiel: UBS-Bank-Fall

Über zwei Milliarden Dollar hat ein Händler der UBS-Bank mit einer unerlaubten Aktion verspielt.

Laut UBS sollen jetzt mögliche Fehler in den internen Kontrollsystemen aufgedeckt werden, die dafür gesorgt haben, dass die Aktivitäten zunächst unentdeckt blieben.

Beispiel: Siemens-Korruptionsaffäre

Siemens stand im Mittelpunkt eines der größten Korruptionsskandale der deutschen Wirtschaftsgeschichte. Die Gesamtkosten mit Strafen, Beraterkosten und Steuernachzahlungen belaufen sich dem Vernehmen nach auf fast drei Milliarden Euro.

Der Bereich Compliance wurde bei Siemens daraufhin völlig neu ausgerichtet

1. Datenschutzkonformes Arbeitnehmerscreening

Arbeitnehmerscreening in der Form der automatisierten Prüfung bestimmter Daten zu Mitarbeitern oder eines Abgleichs verschiedener Datenbestände gegeneinander kann ein geeignetes Mittel sein, Compliance-Verstöße aufzudecken oder zu verhindern.

Das Persönlichkeitsrecht schützt die Arbeitnehmer vor zu weitgehenden Überwachungsmaßnahmen.

Beispiel: Fall Deutsche Bahn - Massenscreening/Rasterfahndung, Pressemeldung im Januar 2009:

Nach den bekanntgewordenen Informationen hat die Bahn vor dem Verkehrsausschuss des Bundestags zugegeben, in dem Projekt "Babylon" bei 173.000 Mitarbeitern und 80.000 Lieferanten Daten "gescreent" zu haben. Dies hat dann auch zu einem Bußgeldverfahren durch den dafür zuständigen Berliner Datenschutzbeauftragten geführt.

Die genaue Grenzziehung zwischen zulässigem Datenscreening zur Aufklärung bzw. Verhinderung von Rechtsverstößen und überzogener/unzulässiger Mitarbeiterkontrolle ist häufig strittig.

Zur **Aufdeckung** von **Straftaten**, die im Beschäftigungsverhältnis **begangen wurden**, gibt es im Moment die spezielle eingrenzende Regelung in § 32 Abs. 1 Satz 2 BDSG.

Bei **Ordnungswidrigkeiten**, die im Beschäftigungsverhältnis begangen wurden, oder **anderen gewichtigen Regelverstößen bzw. Verfehlungen** ist für Datenscreenings unter Umständen die allgemeine Vorschrift von § 32 Abs. 1 Satz 1 BDSG relevant, wonach die Verwendung von Mitarbeiterdaten **für die Durchführung des Beschäftigungsverhältnisses erforderlich** sein muss.

Diese beiden Regelungen in § 32 Abs. 1 BDSG geben nach verbreiteter Auffassung nur in sehr eingegrenzten Fällen eine Rechtsgrundlage für Datenscreenings von Arbeitnehmerdaten ab.

Anlasslose bzw. verdachtslose oder vorbeugende Massenscreenings von Arbeitnehmerdaten werden allgemein als nicht vom BDSG gedeckt angesehen.

Im bisherigen Entwurf für die BDSG-Änderung (§ 32d Abs. 3 BDSG-E) ist eine gemeinsame Regelungen für die **Aufdeckung von Straftaten und andere schwerwiegende Pflichtverletzungen** im Beschäftigungsverhältnis durch Datenabgleiche vorgesehen. Danach darf in einem ersten Schritt nur ein automatisierter Abgleich von Beschäftigtendaten in anonymisierter oder pseudonymisierter Form erfolgen. Nur in einem sich daraus ergebenden Verdachtsfall in Richtung bestimmter Personen dürfen die Ergebnisse des Datenabgleichs dann personalisiert werden.

Ob ein Screening von Arbeitnehmerdaten unter Verwendung von Pseudonymen für die Identifikationsdaten der Mitarbeiter ein relevantes "Mehr" an Persönlichkeitsschutz für die Arbeitnehmer bewirkt, kann hier in Frage gestellt werden, wenn der Arbeitgeber selbst die Mittel zur Wieder-Personalisierung hat und diese Mittel unschwer einsetzen kann.

Auch werden im Gesetzentwurf "Beschäftigtendaten" ohne weitere Einschränkung genannt. Mehrfach angeregt wurde hierzu, eine Begrenzung auf für die Art der denkbaren Straftaten bzw. schwerwiegenden Pflichtverletzungen **erforderlichen** Beschäftigtendaten einzubauen, um Screenings von vorne herein auf einen eingegrenzten Mitarbeiterkreis zu beschränken.

Als Ergebnis der öffentlichen Anhörung zu dem Gesetzentwurf im Mai 2011 soll noch einschränkend in diese Bestimmung des Entwurfstextes aufgenommen werden, dass als weitere Voraussetzung für ein Datenscreening **vorher ein Risikoanalysesystem** ein konkretes Risiko von bestimmten Straftaten oder anderen schwerwiegenden Pflichtverletzungen ausweist. Der Gesetzgeber wird also möglicherweise doch noch die heftig kritisierten anlasslosen bzw. verdachtsfreien Massenscreenings angehen.

Spezialfall "Terrorlisten-Screening"

Zur Zeit wird intensiv darüber diskutiert, ob und inwieweit die EU-Verordnungen 2580/2001 und 881/2002 eine ausreichende datenschutzrechtliche Grundlage für ein Mitarbeiter-Datenscreening zur Suche nach Terrorverdächtigen abgeben. Insbesondere wer als Unternehmen mit Auslandsbeziehungen den zollrechtlichen Status eines "zugelassenen Wirtschaftsbeteiligten" (sog. AEO-Zertifizierung) in Anspruch nehmen möchte, stellt sich die Frage, in welchen Umfang er ein Terrorlisten-Screening durchführen muss.

Es wäre wünschenswert, wenn der deutsche Gesetzgeber hier für eine Klarstellung sorgen würde, welche Mitarbeiter bei welchen Sachverhalten insoweit zu überprüfen sind.

Das Finanzgericht Düsseldorf sieht in einem Urteil vom 01.06.2011 (Az. 4 K 3063/10 Z) eine datenschutzrechtliche Zulässigkeit nach § 28 Abs. 2 BDSG (zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit) sowie eine Verpflichtung von Unternehmen, die Namen von Bediensteten in sicherheitsrelevanten Bereichen mit den "Terror-Listen" abzugleichen.

2. Instrument Whistle-Blowing

Ein Instrument zur Aufdeckung von (mutmaßlichen) Rechtsverstößen und anderen Missständen in einem Unternehmen sind Informationen aus der eigenen Mitarbeiterschar, z. B. in Form eines sogenannten Whistleblowing-Systems. Regelungen in den USA verpflichten teilweise sogar zum Einsatz solcher Meldeverfahren über Rechtsverstöße, was deutsche Unternehmen mit Beziehungen in die USA direkt berühren kann.

Die arbeitsrechtliche Problematik zeigt die Entscheidung des Europäischen Gerichtshofs für Menschenrechte vom 21.07.2011 (Az.: 28274/08) auf. Der Gerichtshof hat befunden, dass die fristlose Kündigung einer Arbeitnehmerin wegen deren Veröffentlichung von Missständen bei ihrem Arbeitgeber, einem Pflegeheimbetreiber, gegen die Menschenrechtskonvention

verstößt und dass dieser Arbeitnehmerin deswegen ein Schadensersatz von 15.000 € zusteht. In den vorangehenden deutschen arbeitsgerichtlichen Verfahren hatte die Arbeitnehmerin keinen Erfolg; ihr Recht, sich bei dem gegebenen Sachverhalt als Whistleblowerin zu betätigen, war dort anders gesehen worden.

Die Meldung von solchen Verstößen durch die Mitarbeiter wird aus datenschutzrechtlicher Sicht z. B. in einem Arbeitsbericht der Datenschutzaufsichtsbehörden aus dem Jahre 2006 behandelt, vgl. unter

https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/6_Whistleblowing-Hotlines/Whistleblowing-Hotlines.pdf

Kurz vorher hatte sich hierzu auch schon die sogenannte Artikel-29-Datenschutzgruppe der EU in einem Arbeitspapier geäußert (WP 117,

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf).

Fragestellungen dabei sind vor allem der Informantenschutz des Meldenden, der Schutz und die Unterrichtung von (möglicherweise unberechtigt) Beschuldigten sowie durch welche organisatorischen Maßnahmen eine datenschutzgerechte Gestaltung eines Whistleblowing-Systems erfolgen sollte.

Als entscheidend wird von den Datenschützern angesehen, dass die Verfahren zur Meldung von Missständen die vertrauliche Behandlung der Identität des Hinweisgebers sicherstellen, und ihm wegen einer solchen Meldung keine Benachteiligungen drohen.

Mangels einer speziellen datenschutzrechtlichen Regelung zum Whistle-Blowing kann derzeit im BDSG nur auf die allgemeine Vorschrift von § 32 Abs. 1 bzw. eventuell § 28 Abs. 1 BDSG zurückgegriffen werden, was mit vielen Unsicherheiten verbunden ist.

Trotz Anstößen von verschiedenen Seiten, auch von den Datenschützern, hat der Bundestag für das Whistleblowing bisher bei der BDSG-Änderung keine Regelung vorgesehen.

Auch früheren Vorschlägen für eine Whistleblower-Vorschrift im Arbeitsrecht, z. B. in einem neuen § 612a BGB, hatte der Gesetzgeber eine Absage erteilt.

Es bleibt also möglicherweise bei dem nicht konkret geregelten Zustand für Whistleblowing-Instrumente und den Unternehmen kann nur geraten werden, solche Instrumente in enger Abstimmung mit ihrem Datenschutzbeauftragten und der Arbeitnehmervertretung zu gestalten.

3. Grenzen von Ermittlungen

3.1 Beauftragung von Detektiven

Eine Beauftragung von Detektiven durch den Arbeitgeber für die heimliche Überwachung von Mitarbeitern kann nach unserer Auffassung immer nur das letzte Mittel zur Erhebung von Daten sein, wenn für einen konkreten Missbrauchssachverhalt alle anderen Ermittlungsmöglichkeiten ausgeschöpft wurden bzw. erfolglos sind.

Der auch in den Medien umfangreich diskutierte Fall "Lidl" hat die Grenzen sowie das Übermaß beim Einsatz von Detektiven noch einmal deutlich gemacht. Damals wurde auch vor der Privatsphäre von Mitarbeitern nicht halt gemacht und selbst Toilettengänge protokolliert. Bußgeldverfahren in einer Reihe von Bundesländern, auch bei uns, waren die Folge.

Das Amtsgericht Siegburg betont zu einem anderen Sachverhalt in einem Urteil vom 29.09.2004 (Az.: 4 C 805/03):

Ob der Eingriff in das allgemeine Persönlichkeitsrecht durch eine private Observation rechtswidrig ist, ist in jedem Einzelfall durch eine umfassende Güter- und Interessenabwägung festzustellen, in der darüber zu befinden ist, ob berechnete Interessen gegenüber dem Persönlichkeitsrecht des Beobachteten den Vorrang genießen.

Der vorgesehene § 32e BDSG-Entwurf grenzt die verdeckte Erhebung persönlicher Daten, z. B. durch Detektive, aus meiner Sicht angemessen ein, in dem er als Voraussetzung einen durch Tatsachen begründeten Verdacht auf Straftaten oder anderen schwerwiegenden Pflichtverletzungen im Beschäftigungsverhältnis fordert und auch Maßstäbe für ein verhältnismäßiges Vorgehen festlegt. Das planmäßige Überwachung wird einerseits zeitlich eingegrenzt, andererseits werden bestimmte Techniken verboten, wie das Abhören und Aufzeichnen von nicht-öffentlichen Gesprächen.

3.2 Verdeckte Videoüberwachung

Heimliche Videoüberwachung von Beschäftigten haben die Arbeitsgerichte in der Vergangenheit teilweise als Möglichkeit zur Aufklärung von konkreten Straftaten und

anderen schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis akzeptiert, wenn die verdeckte Videoüberwachung praktisch das einzige verbliebene Mittel zur Aufklärung noch ist und dies insgesamt nicht unverhältnismäßig ist.

Im Gesetzentwurf zur BDSG-Änderung sieht § 32f BDSG auch in den firmeninternen Bereichen - wegen der besonderen Schwere des Eingriffs in das Persönlichkeitsrecht - keine Möglichkeit der heimlichen Videoüberwachung vor. Die Kernaussage lautet: Der Arbeitgeber hat den Umstand der Videoüberwachung durch geeignete Maßnahmen erkennbar zu machen.

Dies wird einerseits von manchen Stimmen als die mutigste Vorschrift des Gesetzentwurfs gesehen, andererseits von Arbeitgeberseite heftig als zu eng und praxisfremd kritisiert. Wir warten hier die endgültige Entscheidung des Gesetzgebers ab.

3.3 Verdeckte GPS-Überwachung

Für eine Überwachung von Mitarbeitern mittels **heimlich** eingesetzter GPS-Sender durch den Arbeitgeber sehen wir in den geltenden Vorschriften regelmäßig keine rechtliche Grundlage, weil damit ein das Persönlichkeitsrecht erheblich tangierendes Bewegungsprofil gebildet werden kann.

Selbst staatlichen Strafverfolgungsbehörden sind derartige Maßnahmen zur Gewinnung eines Bewegungsprofils nur unter relativ engen Voraussetzungen nach § 100h StPO (Straftat von erheblicher Bedeutung) erlaubt.

Das Landgericht Lüneburg hat z. B. in einem Beschluss vom 28.03.2011 (Az.: 26 Qs 45/11) für einen Detektiv das verdeckte Anbringen eines GPS-Senders an einem fremden Kraftfahrzeug (zur Aufklärung der Frage von zivilrechtlichen Vertragsverstößen) als **strafbar** nach § 44 Abs. 1 BDSG gesehen.

Das OLG Koblenz sieht in einem Urteil vom 30.05.2007 (Az.: 1 U 1235/06) wegen Verletzung des Rechts auf informationelle Selbstbestimmung einen **Auskunftsanspruch** des Kfz-Besitzers gegenüber einem Detektiv zu dessen Auftraggeber, wenn der Detektiv heimlich ein GPS-Ortungsggerät an dem Kfz angebracht hatte. Das OLG betrachtet den Auftraggeber hier als Mittäter bzw. mittelbaren Handlungsstörer an der unerlaubten Handlung des Detektiv.

Die geplante Neuregelung in § 32g des BDSG-Änderungsentwurfs stellt klar, dass der Einsatz von Ortungssystemen den Beschäftigten erkennbar zu machen ist. In der Bestimmung wird auch festgelegt, für welche Zwecke Ortungssysteme bei Beschäftigten eingesetzt werden dürfen, nämlich wenn dies aus betrieblichen Gründen zur Sicherheit der Beschäftigten oder zur Koordinierung des Einsatzes von Beschäftigten erforderlich ist und in dem betreffenden Sachverhalt keine entgegenstehenden schutzwürdigen Belange der Beschäftigten zu erkennen sind.

Aus meiner Sicht eine datenschutzfreundliche Festlegung.

Von Seiten der Wirtschaft wird die vorgesehene Regelung teilweise als zu eng kritisiert.

3.4 Kontrollen der E-Mail- und Internet-Nutzung

Eine der nach unseren Erfahrungen häufigsten datenschutzrechtlichen Streitfragen in Beschäftigungsverhältnissen, nämlich die Problematik der Zugriffe auf bzw. der Kontrollen von Daten der Internet- und E-Mail-Nutzung von Mitarbeitern **bei erlaubter oder geduldeter Privatnutzung**, wird im Änderungsentwurf zum BDSG bisher leider nur kurz angesprochen.

Nur zum Teil finden sich in der Praxis bisher zureichende betriebliche Regelungen hierzu, z. B. durch eine Betriebsvereinbarung oder eine sonstige klare Organisationsverfügung des Arbeitgebers.

Die Problemfälle sind hier vielgestaltig, und reichen von der Aufklärung von Missbrauchsfällen anhand der protokollierten Internet- und E-Mail-Nutzungen über die allgemeinen Zugriffsfragen von Vorgesetzten oder Stellvertretern auf fremde E-Mail-Accounts bis zum richtigen Vorgehen beim plötzlichen Ausfall eines Mitarbeiters.

Der bisherige § 32i des Entwurfstextes befasst sich schwerpunktmäßig mit der beruflichen bzw. dienstlichen Nutzung von Telekommunikationseinrichtungen und enthält lediglich in Absatz 4 Satz 2 die Festlegung, dass der Arbeitgeber private Daten und Inhalte nur erheben, verarbeiten und nutzen darf, wenn dies zur Durchführung des ordnungsgemäßen Dienst- oder Geschäftsbetriebs unerlässlich ist und er den Beschäftigten hierauf schriftlich hingewiesen hat. Dies soll vor allem Weiterleitungsfälle bei Abwesenheit betreffen, lässt aber eine Reihe von weitergehenden Auslegungen zu.

Hier bleiben nach verbreiteter Meinung viele Fragen offen und es wäre zu wünschen, wenn in diesem Punkt der Zugriffe auf E-Mail-Accounts sowie auf die Protokollierungen der Technik-

Nutzungen auch bezüglich der privaten Verwendung dienstlicher Mittel noch eine Klärung im BDSG erfolgen würde.

Ist z. B. der Arbeitgeber bei erlaubter Privatnutzung damit TK-Diensteanbieter im Sinne des TKG bzw. wie weit geht die Reichweite des Fernmeldegeheimnisses?

Bestehen Einwilligungsmöglichkeiten der Mitarbeiter bei Privatnutzung in notwendige Überwachungs- und Zugriffsmöglichkeiten für den Arbeitgeber?

Mögliche Regelungen durch Betriebsvereinbarung?

usw.

4. § 42a BDSG, Meldepflichten bei Datenpannen.

Der geplante § 32j des BDSG-Entwurfs schafft für Beschäftigtendaten eine spezielle Regelung zu Mitteilungspflichten an die Betroffenen und die Datenschutzaufsichtsbehörde bei sogenannten Datenpannen. Damit wird die allgemeine Regelung des zum 01.09.2009 in Kraft getretenen § 42a BDSG erweitert. Es geht dabei um Sachverhalte, in denen Beschäftigtendaten entweder unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.

Nach § 32j BDSG-E sind die Betroffenen bei jeder Datenpanne mit beim Arbeitgeber gespeicherten Beschäftigtendaten zu informieren, und nicht nur, wie im geltenden § 42a BDSG, wenn zusätzlich aufgrund der Datenpanne schwerwiegende Beeinträchtigungen der Rechte oder schutzwürdigen Interessen der Beschäftigten drohen.

Datenpannen sind nach unseren bisherigen Praxiserfahrungen hauptsächlich

- die Fälle von Hacking in DV-Systemen,
- gestohlene und verlorengegangene mobile DV-Gerätschaften sowie
- unzulässige Datenübermittlungen, wie Fehlversendungen oder versehentliche Veröffentlichungen.

Aus dem Bereich der Beschäftigtendaten hatten wir z. B. folgende Datenpannen aufzuarbeiten:

- Diebstahl von zwei Notebooks mit unverschlüsselten Personaldaten zu etwa 5000 Mitarbeitern;

- versehentliche Veröffentlichung von Beschäftigtendaten/Bewerbungsdaten im Internet;
- Fehlversendungen von Personalunterlagen wegen Adressierungs- und Kuvertierungsproblemen.

Für uns geht es dabei im ersten Schritt um die Maßnahmen zum Schutz der durch die Datenpanne betroffenen Personen, im zweiten Schritt um eine vollständige Klärung der Ursachen der Datenpanne und drittens um eine Sicherstellung durch geeignete Maßnahmen, dass künftige Datenpannen vermieden werden.

Ein Kritikpunkt aus meiner Sicht an dem § 32j BDSG-E, wie übrigens auch am geltenden § 42a BDSG, ist die Tatbestandsvoraussetzung "Stellt der Arbeitgeber fest...".

Diese Formulierung führt gerade bei gestohlenen oder verlorengegangenen Datenträgern zu Auslegungsproblemen, wann beim Arbeitgeber von einer solchen Feststellung auszugehen ist, dass Beschäftigtendaten auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.

Aus meiner Sicht kann ein Arbeitgeber bei verlorengegangenen oder gestohlenen Datenträgern nicht abwarten, ob z. B. ein Schaden durch Missbrauch von Kontodaten mittels illegaler Lastschriftabbuchungen eintritt und dann erst diese im Gesetz vorgesehene "Feststellung" treffen sowie darauf hin die Mitteilung an Betroffene und die Aufsichtsbehörde durchführen. Dies würde dem Schutzzweck der Vorschrift zuwider laufen.

Ich meine daher, dass der Tatbestand im Gesetzentwurf -und auch im bestehenden § 42a BDSG- anders formuliert werden sollte, wie z. B. "Hat ein Arbeitgeber Anhaltspunkte dafür...".

5. Resümee

Die vielen Meinungsäußerungen und Kritiken an dem Gesetzentwurf zeigen, dass es hier um Fragen geht, die die Menschen in der Arbeitswelt sehr bewegen.

Hier sollte ohne Zeitdruck sorgfältig geprüft und abgewogen werden.