

Arbeitnehmerdatenschutz

1. Einleitung

Die Debatte um Datenschutz und Datensicherheit hat Konjunktur. Obgleich die aktuellen parlamentarischen Verfahren allenfalls als erste Schritte in die richtige Richtung gewertet werden können, bewegt sich endlich etwas in der deutschen Datenschutzlandschaft. Die Etablierung eines Datenschutzauditsiegels, die gesetzliche Normierung der OptInLösung oder die Beschränkung der Zulässigkeit sog. Scoringverfahren seien hierfür exemplarisch genannt.

Der Arbeitnehmerdatenschutz hingegen sieht sich in diesem Zusammenhang einer geradezu stiefmütterlichen Behandlung ausgesetzt; obgleich der Deutsche Bundestag die Bundesregierung mehrfach aufgefordert hat, den Schutz von Arbeitnehmerdaten zu verbessern und hierzu fraktionsübergreifende Entschlüsse vorgelegt hat, hat es gesetzgeberische Aktivitäten bislang nicht gegeben.

Dabei liegt die Notwendigkeit der Schaffung klarer Strukturen für diesen Bereich auf der Hand: Gerade während eines Beschäftigungsverhältnisses sammeln sich umfangreiche personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter an, deren Verarbeitung in ganz überwiegendem Maße in automatisierter Form erfolgt. Dies gilt sowohl für privatrechtliche Anstellungsverhältnisse als auch für Beschäftigungsverhältnisse im öffentlichen Dienst.

Zudem haben nicht zuletzt die jüngsten Vorfälle im Einzelhandel gezeigt, dass die verdeckte Überwachung am Arbeitsplatz mittels Videotechnik nicht auf einzelne Fälle beschränkt bleibt. Die Bewertung dieser Sachverhalte anhand der geltenden landes- und bundesdatenschutzrechtlichen Vorschriften erweist sich dabei oftmals als schwierig und unübersichtlich. Sowohl Arbeitgeber als auch Arbeitnehmer werden auf eine Analyse der bestehenden Rechtsprechung verwiesen, die indes regelmäßig einzelfallbezogen ist und allenfalls nur von einem kleinen Expertenkreis überblickt wird.

Zwischen Arbeitnehmern und Arbeitgebern besteht oftmals kein gleichberechtigtes Verhältnis. Arbeitnehmer machen nicht selten wegen der mangelnden Kenntnis der Rechtslage von den ihnen bereits jetzt bei Verstößen gegen datenschutzrechtliche Bestimmungen zur Verfügung stehenden Möglichkeiten keinen Gebrauch. Darüber hinaus droht die Situation einzutreten, dass Arbeitnehmer aus Angst vor Repressionen oder gar dem Verlust des Arbeitsplatzes auf die Geltendmachung eigener Rechte bewusst verzichten.

Die Ausgestaltung der Rahmenbedingungen gerade eines so vielgestaltigen Themenbereiches der Judikatur zu überlassen, erscheint als der falsche Weg. Arbeitnehmerdatenschutz ist nicht Sache des Bundesarbeitsgerichts, sondern allein des Gesetzgebers. Ein gesetzgeberisches Handeln ist insoweit längst überfällig. Nur ein umfassendes Arbeitnehmerdatenschutzrecht wird dem Schutz der Persönlichkeitsrechte der Arbeitnehmer gerecht.

Die Vorgabe, die datenschutzrechtlichen Belange der Arbeitnehmer und der Beschäftigten im öffentlichen Dienst zu stärken und transparenter auszugestalten, hat sich die Arbeitsgemeinschaft Arbeitnehmerdatenschutz zum Ziel gesetzt. Eingesetzt vom Landesvorstand der FDP in Nordrhein-Westfalen wirkten hieran unter dem Vorsitz von Gisela Piltz die folgenden Personen mit: Marco Biewald, Karl-Peter Brendel, Prof. Peter Gola, Dr. Dr. h.c. Burkhard Hirsch, Dr. Joachim Jacob, Andreas Jaspers, Alexander May LL.M., Dr. Robert Orth, Jan Schiller und Dr. Matthias Schulenberg.

Im Rahmen der Arbeitsgemeinschaft wurden insbesondere die einzelnen Abschnitte des Beschäftigungsverhältnisses auf ihre datenschutzrechtliche Relevanz hin untersucht und die nachfolgenden Punkte für verbesserte Regelungen erarbeitet. Die erarbeiteten Grundsätze sollen vorbehaltlich besonderer beamtenrechtlicher Bestimmungen, auch für Beamte und Angestellte des öffentlichen Dienstes gelten. Soweit keine besonderen Bestimmungen für den Arbeitnehmerdatenschutz getroffen werden, gelten die Bestimmungen des BDSG und des BetrVG. Die vorgelegten Eckpunkte sollen nunmehr als Arbeitsgrundlage für eine breite Diskussion mit weiteren Experten und Verbänden dienen. Der Landesvorstand wird beauftragt, im Nachgang die hierbei gewonnenen Erkenntnisse auszuwerten.

2. Liberale Thesen

2.1. Bewerbung / Einstellung

• Grundsätzliches

- ✓ Die Daten müssen grundsätzlich beim Betroffenen erhoben werden.
- ✓ Hinsichtlich der zulässigen Fragen an Bewerber ist die geltende Rechtslage ausreichend. Sie sollte aber kodifiziert werden. Unzulässige Fragen dürfen weder dokumentiert noch gegenüber den Betroffenen oder Dritten durch den potentiellen Arbeitgeber verwendet werden.
- ✓ Öffentlich zugängliche Daten über den Bewerber können zur Kenntnis genommen werden (Erlangung von Spezialkenntnissen durch Nutzung von Angeboten, die einer Registrierung bedürfen, wie z.B. XING).
- ✓ Das Verbot der automatisierten Einzelentscheidung (bisher § 6a BDSG), das insbesondere bei psychologischen Auswahltests eine Rolle spielen kann, soll im Arbeitsrecht eindeutig festgeschrieben werden.

• Einstellungs- und weitere Untersuchungen

- ✓ Untersuchungen, die keine Aussage zur Leistungsfähigkeit des Arbeitnehmers bzgl. der konkreten Tätigkeit zulassen, dürfen nicht vorgenommen werden.
- ✓ Gentests oder Fragen zu genetischen Dispositionen sollen grundsätzlich ausgeschlossen werden.
- ✓ Bei gefahrgeneigter Tätigkeit soll es zum Schutz Dritter, des Arbeitgebers und des Arbeitnehmers selbst möglich sein, regelmäßige Untersuchungen durchzuführen. Diese Untersuchungen sollen allerdings nur möglich sein, wenn sie für die Eignung der Tätigkeit zwingend notwendig sind (z.B. Alkoholtest bei Lkw-Fahrer).

2.2. Das laufende Beschäftigungsverhältnis

• Umgang mit Bewerbungsunterlagen

- ✓ Bewerbungsunterlagen auf Stellenausschreibungen sind dem Bewerber zurückzusenden. Bewerberdaten sind auf jeden Fall zu löschen. Im Falle einer erfolglosen Bewerbung dürfen Daten nur so lange aufbewahrt werden, wie dies rechtlich geboten ist, z.B. im Hinblick auf das Allgemeine Gleichbehandlungsgesetz (AGG). Wird eine längere Aufbewahrung seitens des Arbeitgebers gewünscht, setzt dies das Einverständnis des Bewerbers voraus.

• Personalakte

- ✓ Zur Personalakte gehören alle Unterlagen und Vorgänge, die in einem unmittelbaren inneren Zusammenhang mit dem Beschäftigungsverhältnis des Mitarbeiters stehen. Zur Personalakte gehören daher auch alle schriftlichen Aufzeichnungen, die sich mit der Person des Arbeitnehmers und dem Inhalt und Verlauf seines Beschäftigungsverhältnisses befassen. Es ist dabei nicht entscheidend, wo, in welcher Form und unter welcher Bezeichnung die Daten gespeichert sind.
- ✓ Wer Personalentscheidungen zu treffen hat, dem stehen die für eine sachgerechte Entscheidung erforderlichen Unterlagen zur Verfügung. Der Kreis der Zugriffsberechtigten ist möglichst klein zu halten. Bei elektronischer Aktenführung muss die Zugriffsberechtigung geregelt werden. Betriebsräte haben nur mit Zustimmung des Betroffenen Einsicht in die Personalakte. Auf Stammdaten können der Dienstvorgesetzte und der Betriebsrat zugreifen.
- ✓ In die Personalakte dürfen nur konkrete korrekte Informationen/Daten aufgenommen werden. Andernfalls stehen dem Betroffenen gegen die entsprechenden Inhalte/Daten unabhängig von der

Art der Verarbeitung neben dem bestehenden arbeitsrechtlichen Recht der Gegendarstellung Abwehrrechte nach dem BDSG (Löschung, Berichtigung, Auskunft, Sperrung) zur Verfügung.

• **Weitergabe von Arbeitnehmerdaten an Dritte**

- ✓ Die Übermittlung von Arbeitnehmerdaten an Dritte ist ohne Einwilligung des betroffenen Mitarbeiters nur dann zulässig, wenn ein „gravierendes Interesse“ an der Durchbrechung des Grundsatzes der Vertraulichkeit besteht. Ein solches gravierendes Interesse kann z.B. bei Unternehmensverkäufen bestehen.
- ✓ Bei einem Unternehmensverkauf mit „Due Diligence Prüfungen“ dürfen Daten nur anonymisiert weitergegeben werden. Daten von Angestellten i.S.v. § 5 Abs. 2 bis 4 BetrVG dürfen jedoch weiter gegeben werden.
- ✓ Ein europaweites Konzernprivileg ist grundsätzlich möglich. Über Europa hinaus soll ein Konzernprivileg nur dann möglich sein, wenn ein vergleichbares Datenschutzniveau besteht und die Rechte des Betriebsrates – nämlich die Einhaltung der gesetzlichen Voraussetzungen zu prüfen – erhalten bleiben.

• **Whistleblowing**

- ✓ Für das so genannte Whistleblowing sind besonderen Regelungen notwendig. Die allgemeinen Grundsätze und Regelungen (§ 241 BGB – allgemeine Pflichten aus dem Schuldverhältnis) sind dafür nicht ausreichend.

• **Zugangskontrollen und biometrische Daten**

- ✓ Biometrische Daten dürfen nur zu dem Zweck verwendet werden, für den sie ursprünglich erhoben wurden. Zweckänderungen sind unzulässig.
- ✓ Zugangskontrollen sollen grundsätzlich nur der Identitäts- und Anwesenheitskontrolle dienen.
- ✓ Die Arbeitnehmer müssen darüber informiert werden, welche Daten gespeichert werden.
- ✓ Lösungen, bei denen die gespeicherten Referenzdaten unter der alleinigen Kontrolle der Betroffenen stehen und ausschließlich zum Vergleich verarbeitet werden (datensparsame Templates), sind vorzuziehen.
- ✓ Nichtdiskriminierende Ausweichmöglichkeiten sind grundsätzlich vorzusehen, da ein ausnahmsloser Benutzerzwang gegen das Recht auf informationelle Selbstbestimmung verstoßen kann.
- ✓ Insbesondere lassen sich grundsätzlich biometrische Verfahren, die der Verifikation dienen, mit einer dezentralen Datenspeicherung betreiben (1:1 Abgleich).
- ✓ Es müssen detaillierte Zugriffskonzepte geschaffen werden, um eine zweckwidrige Nutzung zu vermeiden und die Daten vor unberechtigtem Zugriff und vor Diebstahl zu schützen.
- ✓ Eine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten ist zu etablieren.
- ✓ Biometrische Daten sollen innerhalb festgesetzter Fristen gelöscht werden. Die Löschung muss überprüfbar sein.

• **Arbeitnehmerüberwachung per Video und permanente Systeme zur Überwachung der Leistungsfähigkeit**

- ✓ Heimliche Videoüberwachungen sind grundsätzlich nicht gestattet.
- ✓ Neben dem im Einzelfall berechtigten Einsatz spezieller Überwachungssysteme dürfen Videoüberwachungssysteme oder andere permanente technische Systeme mit vergleichbarer

Eingriffsintensität (RFID, GPS) nicht zu Zwecken der Leistungs- und Verhaltenskontrolle, zum Leistungsvergleich oder zur Leistungsbemessung eingesetzt werden. Dies gilt insbesondere für Verfahren des Dataminings oder Screenings.

- ✓ Die Überwachung von Produktionsabläufen zur Einhaltung gewerblicher Auflagen sowie von Kassen und sonstigen öffentlich zugänglichen Geschäftsbereichen soll möglich bleiben.
- ✓ Vor dem Einsatz von Videoüberwachung oder anderen permanenten technischen Systemen mit vergleichbarer Eingriffsintensität ist eine Vorabkontrolle des Systems durch den betrieblichen Datenschutzbeauftragten durchzuführen.
- ✓ Die Überwachung von einzelnen Beschäftigten mittels Videoüberwachung und Aufzeichnungssystemen oder anderen permanenten technischen Systemen mit vergleichbarer Eingriffsintensität ist grundsätzlich untersagt, ebenso wie Videoüberwachung, die die Intimsphäre der Arbeitnehmer verletzt (z.B. Toilette und Umkleidekabinen).
- ✓ Auswertungen von Videoaufzeichnungen oder anderen permanenten technischen Systemen mit vergleichbarer Eingriffsintensität dürfen bei konkretem Anlass zur Aufklärung oder Verhinderung von Straftaten genutzt werden und sind zu protokollieren.
- ✓ Aufzeichnungen sind unverzüglich zu löschen, wenn sie nicht mehr erforderlich sind oder schutzwürdige Interessen der Beschäftigten entgegenstehen.
- ✓ Unzulässige Videoaufzeichnungen oder Dokumentationen anderer permanenter technischer Systeme mit vergleichbarer Eingriffsintensität dürfen nicht gegen den Betroffenen verwendet werden.

• **Überwachung von Internet-, Email- und Telefonnutzung (Informations und Kommunikationstechnik)**

- ✓ Auch bei dienstlicher Nutzung von z.B. E-Mail, Internet oder Telefon ist eine Auswertung, die die systematische Kontrolle des Beschäftigten zum Ziel hat, unzulässig.
- ✓ Möglich sind daneben lediglich stichprobenhafte und zeitnahe Auswertungen zu Protokolldaten. Dabei ist ein transparentes Verfahren sicher zu stellen.
- ✓ Straf- und Ordnungswidrigkeitsvorschriften sind entsprechend anzupassen.
- ✓ Die Arbeitnehmer sind über die Inhalte und Details von Protokolldaten zu informieren. Lösungsfristen sind vorzusehen.
- ✓ Eine technische Überwachung des digitalen Arbeitsplatzes ohne Kenntnis der Arbeitnehmer darf grundsätzlich nicht durchgeführt werden.
- ✓ Der Arbeitgeber ist nicht verpflichtet, die private Nutzung von E-Mails, Internet und Telefon zu gestatten oder als sozialadäquates Verhalten zu dulden.
- ✓ Soweit der Arbeitgeber die private Nutzung von Informations- und Kommunikationstechnik gestattet, hat er für den Schutz der Privatsphäre des Arbeitnehmers Sorge zu tragen.
- ✓ Eine flächendeckender Abgleich von Emailkommunikationsdaten widerspricht dem Grundsatz der Verhältnismäßigkeit und ist grundsätzlich ausgeschlossen. Organisatorische Maßnahmen, wie z.B. die Formulierung von Verhaltenskodizes, sind vorzuziehen. Nur im Einzelfall kann ein erheblich überwiegendes Interesse des Arbeitgebers gegeben sein, eine Auswertung der Emailkorrespondenz des Arbeitnehmers vorzunehmen. Denkbar sind hierbei konkrete sich verdichtende Verdachtsmomente, die auf die Begehung einer nicht nur unerheblichen Pflichtverletzung des Arbeitnehmers hinweisen, z.B. Verdacht auf Korruption. Der Betriebsrat ist in etwaige Ermittlungsmaßnahmen einzubeziehen. Die Betroffenen sind im Nachhinein über den erfolgten Abgleich zu informieren.

2.3. Arbeitnehmerdatenschutz und betriebliche Mitbestimmung

- ✓ Der Betriebsrat muss datenschutzrechtliche Belange der Arbeitnehmerinnen und Arbeitnehmer wahrnehmen können. Dies gilt insbesondere vor dem Hintergrund des bestehenden Abhängigkeitsverhältnisses zwischen Arbeitnehmer und Arbeitgeber, das nicht zu einer „datenschutzrechtlichen Abhängigkeit“ des Arbeitnehmers führen darf, z.B. diesen zur Zustimmung zu Erhebung, Nutzung und Verarbeitung von Daten zu bewegen.
- ✓ Die Mitbestimmungsregeln zugunsten des Betriebsrates dürfen nicht dazu führen, dass der einzelne Arbeitnehmer übergangen wird, z.B. wenn es um die Zustimmung zu Überwachungsmaßnahmen geht. Das Allgemeine Persönlichkeitsrecht ist ein höchstpersönliches Rechtsgut und darf nicht der alleinigen Disposition eines Kollektivorgans unterworfen werden.
- ✓ Eine Informationspflicht des Arbeitgebers gegenüber den Betriebsräten im Hinblick auf Arbeitnehmerdatenverarbeitung außerhalb der Personalverwaltung ist zu etablieren.
- ✓ Die Beachtung datenschutzrechtlicher Bestimmungen und die Sanktionierung von etwaigen Verstößen muss auch in Betrieben sichergestellt werden, die nicht über einen Betriebsrat verfügen. An die Verletzung der Unterrichtungspflicht an den betrieblichen Datenschutzbeauftragten muss eine unmittelbare Rechtsfolge geknüpft sein.
- ✓ Transparenz im Mitbestimmungsrecht soll gefördert werden, wobei eine unnötige Behinderung des Produktivgeschäftes vermieden werden sollte.
- ✓ Eine Informationspflicht für den Fall der Datenverarbeitung im Auftrag, auch im Bereich der Personalverwaltung, ist zu etablieren.

2.4. Umgang mit Daten des Arbeitnehmers nach Beendigung des Beschäftigungsverhältnisses

- ✓ Soweit Daten der Arbeitnehmer nicht mehr zur Sicherung von Rechtspositionen benötigt werden, sind diese umgehend und umfassend zu löschen.
- ✓ Dem ausgeschiedenen Arbeitnehmer muss die Möglichkeit eröffnet werden, den Löschvorgang einzusehen und nachvollziehen zu können.
- ✓ Soweit gesetzliche oder vertragliche Vorgaben eine umgehende Löschung verbieten, sind die verbleibenden Daten nur für diese konkreten Vorgaben zu verwenden. Eine anderweitige Nutzung ist ausgeschlossen.
- ✓ Nach Ablauf der Aufbewahrungsfristen sind vorhandene Unterlagen einer ordnungsgemäßen Entsorgung (nach DIN 32757 Stufe 3) zuzuführen. Die Entsorgung ist zu dokumentieren.
- ✓ Die Verarbeitung gesperrter personenbezogener Daten ist grundsätzlich untersagt.