BUNDESARBEITSKAMMER
PRINZ EUGEN STRASSE 20-22
1040 WIEN
T 01 501 65
www.arbeiterkammer.at
DVR 1048384

Bundeskanzleramt Verfassungsdienst
Ballhausplatz 2
1014 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
BKA-810.026/0001-V/3/2012	BAK/KS-GSt/DZ	Daniela Zimmer Gerda Heilegger	DW 2722 DW 2724	DW 2693	10.08.2012

Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2012)

Sehr geehrte Damen und Herren!

Die Bundesarbeitskammer (BAK) bedankt sich für die Gelegenheit, zum übermittelten Gesetzesentwurf wie folgt Stellung zu nehmen:

1. Zusammenfassung der wichtigsten Anliegen:

- **Die Datenschutzbehörde ist finanziell wie personell auf einen zeitgemäßen Stand zu bringen. Damit könnte von Einsparungsmaßnahmen im Informations- und Kontrollsektor der Behörde, wie sie der Entwurf - nicht zuletzt aufgrund von Personalengpässen - vorsieht, Abstand genommen werden.**

- **Ein Rückbau der Vorabkontrollpflichten der Datenschutzbehörde (bei Informationsverbundsystemen; strafrechtlich relevanten Datennutzungen, bei Vorliegen ausdrücklicher Zustimmung der Betroffenen, großteils Videoüberwachung) wird entschieden abgelehnt. Der EU-Trend zu stärkerer Verantwortlichkeit der datenverarbeitenden Unternehmen sollte nicht dazu führen, dass heikle Datennutzungen keiner ex ante-Prüfung mehr unterzogen werden.**

- **Die Einführung von Datenschutzbeauftragten auf freiwilliger Basis wird grundsätzlich begrüßt. Bevorzugt wird allerdings ihre verbindliche Einrichtung.**

Solange das Zusammenwirken zwischen der Datenschutzbehörde und den Datenschutzbeauftragten nicht näher geregelt ist, sollte von einer Privilegierung von Unternehmen mit Datenschutzbeauftragten (Meldebefreiung, Entfall der Vorabkontrolle) Abstand genommen werden. Das derzeitige Konzept verlagert Informations- und Kontrollpflichten in die Betriebe, verspricht aber den Betroffenen noch zu wenig Schutz im Fall der Nichterfüllung sämtlicher von der Behörde auf die Unternehmen übertragenen Aufgaben.

- **Meldebefreite Standardanwendungen sollten weiterhin vom Verordnungsgeber präzise beschrieben werden (Datenarten, maximale Speicherdauer etc).**

2. Allgemeines zum Entwurf

Eingangs sei angemerkt, dass Datenschutzbehörden den Herausforderungen fortschreitender Technologieentwicklung und ihrem Gefährdungspotential für die Privatsphäre nur gewachsen sein werden, wenn sie dem zunehmenden Anforderungsprofil entsprechend personell massiv gestärkt werden. Vor diesem Hintergrund bedauern wir sehr, dass sich ein zeitgemäßer Ausbau der Behörde in Österreich auch weiterhin nicht abzeichnet.

Bereits mit der DSG-Novelle 2010 wurde die Maxime einer starken **Entlastung der Datenschutzbehörde** durch Vereinfachung des Registrierungsverfahrens verfolgt. Kern der neuen Regelungen war die Einführung einer automationsunterstützten Prüfung der eingegangenen Meldungen von Datenanwendungen auf Vollständigkeit und Plausibilität. Die BAK hat in ihrer damaligen Stellungnahme zwar grundsätzlich Verständnis für das Vorhaben signalisiert, gleichzeitig aber die Sorge geäußert, dass mit dem Umstieg auf eine rein automatisierte Kontrolle sich die Anzahl fehlerhafter Meldungen vergrößern könnte bzw gemeldete Datenanwendungen, die dem Datenschutzrecht widersprechen, über einen langen Zeitraum hinweg nicht auffallen dürften.

Auch der nun vorliegende Entwurf ist vom Leitgedanken, Einsparungen zu erzielen, getragen. Wie die Erläuterungen zu den finanziellen Auswirkungen des vorliegenden Entwurfs zeigen, wurden diese Potentiale vor allem im Bereich der Registrierung und Vorabkontrolle durch die Datenschutzkommission identifiziert, also jene Rechtsbereiche, die den Betroffenen, Information und präventiven Schutz versprechen.

Aus Sicht der BAK ist nochmals zu betonen, dass zeitgemäßer Datenschutz zusätzliche finanzielle Investitionen in Informations-, Aufsichts- und Rechtsschutzinstrumente erfordert. Zu den Datenschutzbedürfnissen der Bevölkerung - insbesondere jenen der ArbeitnehmerInnen und KonsumentInnen – zählt insbesondere auch eine wirksame ex ante - Kontrolle von aus Datenschutzsicht heiklen Datenanwendungen. Ein Einschreiten erst im Falle von Beschwerden einzelner Betroffener oder offenkundig gewordener Datenschutzverletzungen kommt naturgemäß zu spät und kann daher keinen ausreichenden Schutz sicherstellen.

Aufgrund der typischen, strukturellen Unterlegenheit der Betroffenen gegenüber Unternehmen, die Auftraggeber von Datenanwendungen sind (keine technischen und rechtlichen Kenntnisse; Abhängigkeitsverhältnisse als ArbeitnehmerIn oder mangelnder Einblick als KonsumentIn in die Datenverarbeitungsprozesse eines Unternehmens uvm) können sich die Betroffenen in diesem Bereich auch nur schwer selbst behaupten. Dem Fürsorgegedanken durch behördliche Information über gemeldete Datenanwendungen und Vorabkontrollen kommt deshalb im Bereich des Datenschutzes besondere Bedeutung zu. Das Melderegister gewährleistet zumindest eine gewisse Transparenz und Publizität über alle relevanten Verarbeitungsvorgänge in Österreich und unterstützt damit die Betroffenen in ihrer grundsätzlich benachteiligten Position: sie können von Datennutzungen, die sie tangieren, leicht Kenntnis nehmen.

ArbeitnehmerInnen sowie BetriebsrätInnen haben durch **Einsichtnahme in das Datenverarbeitungsregister** die Möglichkeit, Informationen über die vom/von der ArbeitgeberIn gemeldeten Anwendungen zu erhalten. Die Strafnorm des § 52 Abs 2 Z 1 DSG knüpft unmittelbar an die Datenverarbeitung ohne (korrekte) Erfüllung der Meldepflicht an, was eine rechtssichere Rechtsdurchsetzung ermöglicht, ohne auf diffizile Fragen der Rechtswidrigkeit oder Interessenabwägungen eingehen zu müssen. Der Wegfall dieses von großer Rechtssicherheit ausgezeichneten Sanktionsmittels würde der Belegschaftsvertretung für die Durchsetzung des Datenschutzes im Betrieb wirksame Mittel aus der Hand nehmen. Nicht übersehen werden darf auch, dass im Zuge der Meldung die dazu nach ArbVG erforderlichen Betriebsvereinbarungen vorzulegen sind – was bei Wegfall der Meldepflicht entfallen würde. BetriebsrätInnenen würde somit einerseits die Möglichkeit genommen, die gemeldeten Datenanwendungen in Erfahrung zu bringen (was insbesondere in jenen Fällen relevant ist, wo der/die ArbeitgeberIn der Informationspflicht gem § 91 ArbVG nicht nachkommt) Zudem würde die Motivation für ArbeitgeberInnen wegfallen, sich gesetzeskonform zu verhalten und vor Meldung und Inbetriebnahme der Datenanwendung auch eine entsprechende Betriebsvereinbarung abzuschließen.

Dem Entwurf zufolge wären sämtliche Datennutzungen eines Unternehmens, das auf freiwilliger Basis einen Datenschutzbeauftragten einsetzt, meldebefreit. Interessierte können sich zwar alternativ an die jeweiligen Datenschutzbeauftragten wenden – wie gut organisiert und „niedrigschwellig“ eine derartige Einsichtnahme durch Betroffene gestaltet ist, wird allerdings sehr vom (Organisations-)Willen des jeweiligen Auftraggebers abhängen.

Mit Blick auf die Interessen der Betroffenen ist uns die Weiterführung eines möglichst vollständigen Datenverarbeitungsregisters ein Anliegen. Mit anderen Worten: mit der Zunahme von Meldebefreiungen und Ausnahmen von der Vorabkontrollpflicht wird auch der Anspruch aufgegeben, die Datenanwendungen in Österreich möglichst übersichtlich und vollständig zu erfassen. Damit geht aber nicht nur interessierten ArbeitnehmerInnen und KonsumentInnen sukzessive der Überblick über die Nutzung ihrer Daten verloren, sondern letztlich auch der Datenschutzbehörde. Vor diesem Hintergrund betrachten wir diese Entwicklung als datenschutzrechtlichen Rückschritt.

Der Verlust an Transparenz und Vorabkontrolle könnte durch den Einsatz von Datenschutzbeauftragten in den Betrieben nur unter strengen Kautelen ausgeglichen werden. Die Einführung eines betrieblichen Datenschutzbeauftragten könnte unter Umständen sogar ein wichtiger Schritt in Richtung einer wirksamen Durchsetzung von Datenschutzbestimmungen in der Arbeitswelt und gegenüber KonsumentInnen sein. Allerdings bedürfte es präziser, strikter Vorgaben hinsichtlich des Zusammenwirkens der Beauftragten mit der Datenschutzbehörde und der Aufsicht durch diese.

Als nicht ausreichend muss jedenfalls die Regelung des § 30 Abs 1a gesehen werden, dass der Datenschutzbeauftragte sich beim Verdacht einer Datenschutzverletzung an die Datenschutzkommission wenden *kann*, wenn der Auftraggeber informiert wurde und keine Abhilfe geschaffen wurde. Diese Regelung wäre völlig zahnlos, zumal die Möglichkeit zur behördlichen Anzeige ohnedies jedermann offensteht. Hier wäre jedenfalls eine Verpflichtung zur Meldung vorzusehen, um die Effizienz der Einsetzung von Datenschutzbeauftragten nicht von vornherein zu untergraben.

Unzureichend ist überdies die Möglichkeit der Einsichtnahme von „Betroffenen“ in die beim Datenschutzbeauftragten geführten Meldungen – hier fehlt die Regelung eines Rechtszuges zur Datenschutzkommission für den Fall, dass ein Streit über die Betroffenheit des/r Einsicht Begehrenden entsteht und damit die Einsicht verweigert wird.

Weiters ist zu bezweifeln, dass die vorgesehene Sammlung der betriebenen Anwendungen beim Datenschutzbeauftragten für eine dem Datenverarbeitungsregister vergleichbare Rechtssicherheit sorgt. Es fehlen jegliche Regelungen, die sicherstellen sollen, dass nachträglich Änderungen in das Verzeichnis beim Datenschutzbeauftragten aufgenommen werden.

Der Entwurf enthält bedauerlicherweise keine ausreichenden Garantien, die sicherstellen, dass – neben im Einzelfall durchaus engagierten, unabhängigen Datenschutzbeauftragten – Beauftragte nicht nur pro forma eingesetzt werden, um den Meldepflichten und der Vorabkontrolle zu entgehen. Das vorliegende Konzept eines Zusammenspiels zwischen betrieblicher und behördlicher Datenschutzkontrolle ist aus unserer Sicht somit nicht ausgereift genug, um Auftraggeber, die Datenschutzbeauftragte namhaft machen, durch Entfall der Melde- und Vorabkontrollpflichten derart weitgehend zu privilegieren.

Vor diesem Hintergrund sollte an einen Ersatz des Datenverarbeitungsregisters durch betriebsinterne Mechanismen erst dann gedacht werden, wenn gesetzliche Auflagen und Vollzugsnormen sicherstellen, dass Datenschutzbeauftragte in der Praxis in einer dem Meldeverfahren entsprechenden Weise Transparenz und Rechtskonformität gewährleisten.

3. Zu den Bestimmungen im Einzelnen:

Zu § 17 Abs 2 Z 6 Standardanwendung

Die Erläuterungen führen aus, dass zwecks Entlastung von Datenverarbeitungsregister und Auftraggebern die Standardanwendungen in der entsprechenden Verordnung künftig einfacher ausgestaltet werden können. Entsprechend diesem Vorhaben wurde in Z 6 der Passus gestrichen „ In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen."

Aus BAK-Sicht sollten diese Vorgaben an den Verordnungsgeber keinesfalls entfallen. Sie legen den Mindestumfang an Beschreibung der Datenanwendung fest, die in den Genuss einer Meldebefreiung kommen soll. Ohne die Angabe derartiger Details in der Verordnung bestünde wenig Rechtssicherheit darüber, welche Datennutzungen in der Praxis von der Verordnung noch gedeckt sind und welche nicht. Die bloße Bezeichnung bzw. Kategorisierung des Auftraggebers (Personalverwaltung, Kundendateien etc) kann allein für die Zuordnung zu einer Standardanwendung nicht ausschlaggebend sein. AuftraggeberInnen würde ermöglicht, auch bedenkliche, mit möglichen negativen Auswirkungen für die Betroffenen behaftete Datenarten in die „Standardanwendung" aufzunehmen, ohne dass dies einer Kontrolle unterzogen würde. Die Angabe der zulässigen Datenarten, Speicherhöchstdauer etc in der Verordnung gewährleistet darüber hinaus, dass die gesetzlichen Voraussetzungen tatsächlich erfüllt wird (die Gefährdung von Geheimhaltungsinteressen muss aufgrund der verarbeiteten Datenarten unwahrscheinlich sein). Nicht zuletzt ist der Wegfall einer näheren Umschreibung meldebefreiter Anwendungen durch den Verordnungsgeber auch in Hinblick auf das Legalitätsprinzip des Art 18 B-VG zu überdenken.

§ 17 Abs 7 Meldebefreiung im Falle eines betrieblichen Datenschutzbeauftragten

Dem Entwurf zufolge sind Datenanwendungen nicht meldepflichtig, wenn sie „der Kontrolle eines an die Datenschutzkommission gemeldeten Datenschutzbeauftragten … unterliegen."

Wie in der Einführung ausgeführt, sind Datenschutzbeauftragte ohne ausreichenden Pflichtenkatalog und minutiöse Aufsicht durch Behörden kein angemessener Ersatz für den Informations- und Kontrollverlust, der mit der Meldebefreiung verbunden ist:

- Was passiert etwa, wenn Betroffene nicht umstandslos ins Verzeichnis der Datenanwendungen Einsicht nehmen können (dass es Online zugänglich sein muss, ist bspw im Entwurf nicht verankert)?

- Wer kontrolliert, dass der Datenschutzbeauftragte bei vorabkontrollpflichtigen Anwendungen über restriktive Auflagen sicherstellt, dass Geheimhaltungsinteressen auch gebührend berücksichtigt werden?

- Wie bereits im allgemeinen Teil ausgeführt, bedürfte es zudem dringend der Festlegung eines Procedere (Rechtszug zur Datenschutzkommission) für den Fall, dass die Einsicht nicht (ausreichend) gewährt wird.

Weiters müsste die „Fälschungssicherheit“, dh die Verhinderung nachträglicher Änderungen an den beim Datenschutzbeauftragten verzeichneten Meldungen durch entsprechende Maßnahmen sichergestellt werden.

§ 17 a Datenschutzbeauftragter

Die Einführung eines freiwilligen Datenschutzbeauftragten wird grundsätzlich sehr begrüßt. Wir verweisen allerdings auf vorangegangene Stellungnahmen, in denen BAK-seits ihre verpflichtende Einführung gefordert wurde. Auf die Vorbehalte der BAK, die Einführung eines Datenschutzbeauftragten durch eine generelle Meldefreizeichnung und Ausnahme von der Vorabkontrollpflicht der Datenschutzkommission zu begünstigen, wurde bereits eingangs hingewiesen. **Vorbedingung für diesen Schritt wäre ein verpflichtend enges Zusammenspiel zwischen Behörde und Beauftragten (mit entsprechenden Protokoll- und Berichtspflichten des Beauftragten und Durchgriffsrechten der Behörde),** andernfalls würden bisherige behördliche Pflichten bloß weitgehend unkontrolliert in die Betriebe ausgelagert, mit anderen Worten würde sich diesfalls der Kontrollierte selbst kontrollieren.

In Abs 2 wird die Aufnahme einer Verordnungsermächtigung dringend empfohlen. Die Begriffe Fachkunde und Zuverlässigkeit sind nicht nur unbestimmt genug, um im Verordnungsweg näher geregelt zu werden. Welche rechtlichen und technischen Mindestkenntnisse vorauszusetzen (und zweckmäßigerweise der Datenschutzkommission gegenüber auch nachzuweisen) sind, unterliegt auch einem ständigen Wandel. Bedenkt man, dass der Beauftragte künftig auch in vorabkontrollpflichtigen Bereichen die Datenschutzkommission ersetzen, mithin die Rechtskonformität prüfen und geeignete Auflagen erteilen soll, wird das hohe Anforderungsprofil sichtbar. Einen Mindestausbildungsstandard auch rechtlich abzusichern, wäre wichtig.

Da der Datenschutzbeauftragte eine betriebliche Vertrauensperson in Belangen des Datenschutzes sein soll, in welche Richtung auch § 17a Abs 4 des Entwurfes abzielt, läge es auch nahe, folgende Bestellungs- und Ausübungsbedingungen in Bezug auf Sicherheitsvertrauenspersonen zu übernehmen:

- Die Bestellung bedarf der Zustimmung der zuständigen Belegschaftsorgane bzw Organe der Personalvertretung

- Eine vorzeitige Abberufung von Sicherheitsvertrauenspersonen hat auf Verlangen der zuständigen Belegschaftsorgane bzw der zuständigen Organe der Personalvertretung zu erfolgen.

- Der Auftraggeber hat sicherzustellen, dass dem Datenschutzbeauftragten die zur Erfüllung seiner Aufgaben erforderliche Zeit unter Anrechnung auf seine Arbeitszeit zur Verfügung steht.

In Abs 6 wird zwar angeordnet, dass der Auftraggeber den Datenschutzbeauftragten zu unterstützen hat, indem er ihm bspw „Geräte und Mittel zur Verfügung stellt“. Völlig unerwähnt bleibt allerdings, dass dem Beauftragten auch Zugang zu bzw Einsicht in datenschutzrelevante Unterlagen und Betriebsmittel zu gewähren ist, soll er die Datenschutzkonformität des Betriebes prüfen können.

§ 18 Abs 2 Vorabkontrolle

Die Erweiterung der vorabkontrollpflichtigen Datenanwendungen um solche, die der Risikoanalyse, dem Scoring und der Persönlichkeitsprofile dienen, wird ausdrücklich begrüßt.
Es wird allerdings angeregt, statt der „Bestimmung“ bereits die „Eignung“ zu Bewertungen der Persönlichkeit des Betroffenen genügen zu lassen, da es sonst durch bloße täuschende Vorgabe eines anderen Zweckes allzu leicht wäre, die Schutzbestimmung zu umgehen.

Vor dem Hintergrund eines vorsorgenden Datenschutzes in heiklen Bereichen bestehen allerdings BAK-seits Einwände dagegen, zwei bedeutsame Kategorien von derzeit vorabkontrollpflichtigen Datenanwendungen von der Vorabkontrollpflicht auszunehmen. Es bedarf keiner weiteren Begründung, dass strafrechtlich relevante Daten und Daten, die in Form eines Informationsverbundsystemes benutzt werden, die Geheimhaltungsinteressen der Betroffenen äußerst intensiv berühren. Allein die vielen Auflagen, die im Rahmen der Vorabkontrolle der sogenannten „Banken-Warnliste“ erteilt werden mussten, belegen den Bedarf an einem höheren Schutzstandard beim Betrieb von Informationsverbundsystemen. Es wird auch daran erinnert, dass die Vereinfachungen des Registrierungsverfahrens im Rahmen der letzten DSG-Novelle entscheidend damit begründet wurden, die Masse harmloser Verarbeitungen nur mehr eine automatisierte Plausibilitätsprüfung durchlaufen zu lassen, um sich umso konzentrierter den heiklen Vorabkontrollen annehmen zu können.

Vor diesem Hintergrund lehnt die BAK den Entfall der Vorabkontrolle bei strafrechtlichen Daten und Informationsverbundsystemen entschieden ab.

§ 18 Abs 3 Vorabkontrolle

Ähnlich kritisch wird der Entfall der Vorabkontrolle bei einer ausdrücklichen Zustimmung des Betroffenen gesehen. Die Praxis belegt eindrucksvoll, dass Zustimmungen allzu oft nicht freiwillig und noch seltener (mangels ausreichender Informationen darüber bzw mangelhaften Wissen und Verständnisses des Betroffenen) „in Kenntnis der Tragweite“ erteilt werden.

Vor diesem Hintergrund mutet es lebensfremd an, dem Betroffenen die alleinige Verantwortung über die Aufnahme in eine vorabkontrollpflichtige Anwendung zu überantworten. Denn vielfach wird der Betroffene zwar bereit sein, dass seine Daten verarbeitet werden. Die Rechtskonformität einer Datenanwendung kann er mangels Einsichtsbefugnissen im Einzelnen allerdings nicht einmal theoretisch prüfen, geschweige denn einem übermächtigen Vertragspartner – anstelle der bislang behördlichen Auflagen – irgendwelche Vorgaben machen.

Mit diesem Ausnahmetatbestand wird auch die neu eingeführte Vorabkontrolle für Personenbewertungen vollständig ausgehöhlt. Jede Bonitätsbewertung – egal wie sehr sie in die Datenschutzrechte der Betroffenen eingreift – könnte mit dem Nachweis einer Zustimmung der Vorabkontrolle entzogen werden.

Gerade in typischen Abhängigkeitsverhältnissen wie zB im Bereich der Arbeitsverträge kann von einer wirksamen ausdrücklichen Zustimmung nicht ausgegangen werden (vgl zu Arbeitsverhältnissen ua auch den gleichlautenden Hinweis in Ziffer 13 der Entschließung des EP vom 6.7.2011 zum Gesamtkonzept für den Datenschutz in der EU). Im Zweifel würden sich die Auftraggeber zum Schaden der Betroffenen keiner Vorabkontrolle mehr unterziehen, sondern sich auf das Vorliegen einer ausdrücklichen Zustimmung berufen – solange ihre Unwirksamkeit nicht gerichtlich festgestellt ist.

§ 30 Abs 1a Eingaben des Datenschutzbeauftragten

Die Bestimmung sieht vor, dass sich der Datenschutzbeauftragte beim Verdacht einer Datenschutzverletzung an die Datenschutzkommission wenden kann, soweit er den Auftraggeber informiert hat und dieser keine „geeigneten Maßnahmen des vermuteten rechtswidrigen Zustandes„ getroffen hat.

Diese Anordnung bedürfte grundsätzlich keiner Erwähnung: Anzeigen sind ein „Jedermanns“-Recht. Sollte die Bestimmung eine Verpflichtung nahelegen, sollte „kann“ durch „hat“ ersetzt werden, um diesbezügliche Unklarheiten zu beseitigen. Ob eine Sanktionierung für den Fall vorgesehen ist, dass ein anhaltender Verstoß nicht angezeigt wird, ist auch klärungsbedürftig (nach § 52 ist strafbewehrt, wenn der Datenschutzbeauftragte vorsätzlich nicht auf einen rechtmäßigen Zustand hinwirkt – ob nur gegenüber dem Arbeitgeber oder auch unter Einbeziehung der Behörde bleibt offen).

Die Bestimmung soll den Beauftragten wohl auch zum Handeln ermutigen. Ob die Norm dazu geeignet ist, bleibt allerdings dahingestellt: Wann „geeignete Maßnahmen“ vom Auftraggeber getroffen wurden, eröffnet weite Auslegungsspielräume und bietet dem Beauftragten wenig Rechtssicherheit. Keinerlei Maßnahmen werden vom Auftraggeber wohl auch ergriffen, wenn er die Vermutung seines Beauftragten in Hinblick auf die Rechtswidrigkeit nicht teilt. Klarzustellen wäre, dass auch diesfalls eine Einschaltung der Datenschutzbehörde angezeigt ist.

§ 50 Videoüberwachung

Derzeit bedarf die Videoüberwachung der Vorabkontrolle, d.h. bevor die Videoüberwachung in Angriff genommen werden darf, muss sie bei der Datenschutzkommission gemeldet und von dieser genehmigt werden. Dem Entwurf zufolge soll diese Präventivkontrolle entfallen. Die Erläuterungen verweisen darauf, dass nach EU-Vorgaben Vorabkontrollpflichten nur bestünden, soweit sensible Daten gezielt verwendet werden (bspw bei Videobeobachtung von psychisch erkrankten Personen). Konsequenterweise müsste in § 50 c zumindest auf diese Einschränkung hingewiesen werden.

Da BAK-seits der Entfall der Vorabkontrolle bei strafrechtsrelevanten Daten – wie zuvor ausgeführt – entschieden abgelehnt wird, schließt diese Kritik folglich auch den Bereich der Videoüberwachung mit ein, soweit ihr Zweck die Aufklärung von Straftaten ist.

Wie schon in der Begutachtung zur DSG-Novelle 2012 angeregt, wird zu § 50c Abs 1 wiederholt, dass sich die Vorlagepflicht notwendiger Betriebsvereinbarungen nicht nur auf Betriebsvereinbarungen gemäß § 96a ArbVG, sondern auch auf solche gemäß § 96 ArbVG beziehen sollte, zumal gerade § 96 Abs 1 Z 3 ArbVG Kontrollmaßnahmen im Auge hat, die nach § 50a Abs 5 Satz 2 DSG nach hM durchaus noch erlaubt sein könnten, wenn sie nämlich nicht intentional auf eine Mitarbeiterkontrolle ausgerichtet sind, sondern die Möglichkeit der Mitarbeiterkontrolle nur ein (möglicher) Nebenzweck ist, was aber ausreicht, dass diese Möglichkeit der (selbst primär unbeabsichtigten) Mitarbeiterkontrolle unter § 96 Abs 1 Z 3 ArbVG fällt, dh einer entsprechenden Betriebsvereinbarung bedarf; maW schließt § 50a Abs 5 Satz 2 DSG Videoüberwachungen an Arbeitsstätten nicht generell aus, sodass noch ein vielfältiger Anwendungsbereich für Betriebsvereinbarungen gemäß § 96 Abs 1 Z 3 ArbVG und damit auch für deren Vorlagepflicht verbleibt.

Entsprechend sollte in § 50c Abs 1 DSG auch eine Vorlagepflicht von Einzelzustimmungen von Arbeitnehmern gemäß § 10 Abs 1 AVRAG (als korrespondierende Bestimmung in betriebsratslosen Betrieben) vorgesehen werden.

Im Dienste betroffener ArbeitnehmerInnen und KonsumentInnen hoffen wir, dass unsere Anliegen berücksichtigt werden und stehen für weitere Gespräche jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

VP Johann Kalliauer
iV des Präsidenten
F.d.R.d.A.

Melitta Aschauer-Nagl
iV des Direktors
F.d.R.d.A.