Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)584 F

Karsten Neumann

Landesbeauftragter für den Datenschutz

Mecklenburg-Vorpommern a.D.

19. Oktober 2012

gutachterliche Stellungnahme

zur 83. Sitzung des Innenausschusses

Montag, dem 22.10.2012

Öffentliche Anhörung von Sachverständigen

a)

Vorschlag für eine

Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

KOM(2012)11 endg.; Ratsdok.-Nr: 5853/12

b)

Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen

Der Schutz der Privatsphäre in einer vernetzten Welt

Ein europäischer Datenschutzrahmen für das 21. Jahrhundert

KOM(2012)9 endg.; Ratsdok.-Nr: 5852/12

Ressortbericht BMI 14.02.2012

c)

Antrag der Abgeordneten Dr. Konstantin von Notz, Volker Beck (Köln), Kai Gehring, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

EU-Datenschutzreform unterstützen

BT-Drucksache 17/9166

Inhalt

1. Datenschutz – besser Europäisch

Die Kompetenz der Europäischen Union zur Rechtssetzung im Datenschutz ist prominent bestritten worden, allerdings nicht nur aufgrund der Europäischen Verträge zu Unrecht. Eine supranationale Regelung ist vor allem aufgrund der heutigen Realität moderner Informations- und Kommunikationstechnologien alternativlos.

Das Gesetzgebungsverfahren war bereits bis zur Vorlage des Kommissionsentwurfes ein Vorbild für moderne Gesetzgebung, indem die Evaluierung der Europäischen Datenschutzrichtlinie unter breiter öffentlicher Beteiligung und Einbeziehung des Sachverstandes der Zivilgesellschaft durch transparente Diskussionsprozesse erfolgte. Die mehreren hundert Stellungnahmen[1] machten den Bedarf an Harmonisierung und Modernisierung mehr als überdeutlich. Es bleibt nur zu hoffen, dass diese Form von öffentlicher Debatte auch im weiteren Verfahren beibehalten werden kann.

Deutsche Kritiken an europäischer Kodifizierung eines quasi verfassungsrechtlichen Auftrages, nämlich die Umsetzung der europäischen Grundrechte, verkennen bedauerlicherweise den europäischen Kontext. Der europäische Datenschutzbeauftragte Peter Hustinx beschrieb den materiellen Gehalt des Kommissionsvorschlages sehr passend als „kleiner Schritt für Deutschland, aber ein großer Schritt für Europa“. Gerade in international tätigen deutschen Unternehmen engagierte Datenschützer beklagen zu Recht das Umsetzungsniveau der Datenschutzrichtlinie in den europäischen Mitgliedstaaten, das die Akzeptanz deutscher Umsetzungsbemühungen permanent untergräbt und als Wettbewerbsverzerrung interpretiert wird.

An einer Europäisierung des Schutzniveaus geht aber aus weiteren Gründen kein Weg vorbei: es gibt heute keinen Bereich moderner Informations- und Kommunikationstechnik mehr, der sich nicht nationaler Regelung und Kontrolle entzieht. Hardt- und Software, Netzwerke und Informationsquellen, Kommunikationsmittel und Datenspeicherung sind zumindest grenzüberschreitend, aber in der Regel international. Vor diesem Hintergrund erstaunt die Feststellung in der umfassenden Bewertung des BMI auf RD 5852/12 bei der Prüfung der Vereinbarkeit des Gesetzgebungsaktes mit den Grundsätzen der Subsidiarität und Verhältnismäßigkeit schon, nach der „in dem für den Binnenmarkt weniger relevanten öffentlichen Bereich“ Spielräume bleiben sollen. Der öffentliche Bereich nutzt heute im wesentlichen und weit überwiegend die gleichen Mittel und Kommunikationsnetze, wie der nicht-öffentliche Bereich. Eine Differenzierung macht schon längst keinen Sinn mehr. Auch in der vertikalen Zusammenarbeit zwischen den Behörden erzeugen die gleichen Techniken gleiche Risiken. Soweit materiell-rechtlich besondere Erfordernisse besondere Verarbeitungsregelung erfordern, können diese auf gesetzlicher Ebene jederzeit spezialgesetzlich normiert werden.

kein verfassungsgerichtlicher Schutz?

Die Kritik von Masing[2] an einem von Brüssel drohendem Grundrechteabbau dadurch, dass die Materie dem Schutz des Bundesverfassungsgerichts entzogen werde, kann nur

[1] Die 288 im Rahmen der öffentlichen Konsultation eingegangenen Stellungnahmen unter: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm

[2] http://heise.de/-1407072

unterstützt werden, richtet sich aber an den falschen Adressaten. Es waren die Regierungen der Mitgliedstaaten, die berechtigte Kritiken am Verfassungsvertrag mit dem Vertrag von Lissabon statt durch mehr Demokratie und Integration, mit weniger Demokratie beantworteten und Europa damit in eine tiefe Legitimationskrise stürzten. Der von Masing kritisierte Mangel tritt an der Stelle des Datenschutzrechtes besonders schmerzhaft zu tage, stellt aber ein generelles und nur über die Verträge zu lösendes europäisches Problem dar.

2. Erhalt deutscher Datenschutzstandards

Die berechtigte einhellige Forderung nach einem Erhalt der durch deutsche Gesetzgebung und deutsche Verfassungsrechtsprechung erreichte rechtliche Standards - in vielen Fällen gegen Versuche des Gesetzgebers durchgesetzt, das Recht auf informationelle Selbstbestimmung einzuschränken – darf nicht die vielfältig prognostizierten Mängel an der deutschen Datenschutzpraxis und deren Modernisierungsbedarf unterschlagen. So sei daran erinnert, dass die Europäische Kommission bereits die Umsetzung formaler Unabhängigkeitsvorgaben der Aufsichtsbehörden nur durch ein aufwändiges Klageverfahren gegen den Willen der Bundesregierung durchsetzen musste. Daneben gibt es aber bereits nach heutigem Stand der europäischen Datenschutzrichtlinie eine Reihe weiterer Umsetzungsdefizite, von den nicht umgesetzten Richtlinien mit datenschutzrechtlichem Bezug – zum Beispiel die sog. Cookie-Richtlinie[3] - ganz zu schweigen.

Auch in Deutschland sind weiterhin erhebliche Umsetzungsdefizite zu beklagen: sowohl in der Praxis der nicht-öffentlichen Stellen im Umgang mit personenbezogenen Daten, als auch im öffentlichen Bereich. Diese Defizite werfen berechtigte Fragen nach der Effektivität der Datenschutzaufsicht, aber auch nach der Geeignetheit materiell-rechtlicher Vorgaben auf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich vor diesem Hintergrund im Jahr 2010 mit einer bisher unbeantwortet gebliebenen Initiative zur umfassenden Modernisierung des deutschen Datenschutzrechts[4] gewandt und eine Fülle konkreter Vorschläge unterbreitet. Bedauerlicherweise fehlte es bisher am politischen Willen, sich ernsthaft mit den Herausforderungen zu befassen.

[3] PROPOSAL FOR A EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE CONCERNING THE PROTECTION OF PERSONAL DATA AND PRIVACY IN THE CONTEXT OF PUBLIC DIGITAL TELECOMMUNICATIONS NETWORKS, IN PARTICULAR THE INTEGRATED SERVICES DIGITAL NETWORK (ISDN) AND PUBLIC DIGITAL MOBILE NETWORKS, COM (1990) 314 - 5, vgl. http://heise.de/-1204788

[4] Eine Chronologie der Vorschläge unter http://www.bfdi.bund.de/DE/Schwerpunkte/ModernisierungDS/ArtikelNational/Chronologie.html

3. zu a) Datenschutz-Grundverordnung

Demgegenüber hat die Kommission mit ihrem Vorschlag versucht, ein umfassendes Konzept für einen datenschutzrechtlich umfassenden Rechtsrahmen zu entwerfen, das grundsätzlich geeignet ist, europaweit ein einheitlich hohes Datenschutzniveau zu erreichen. Deutschland sollte vor dem Hintergrund dieser Zielstellung die Kommission unterstützen und für europaweit für die angestrebte Verordnung werben. Schon aufgrund des vergleichsweise hohen Niveaus der Datenschutzpraxis in deutschen Unternehmen und der großen Deckungsgleichheit deutscher Regelungen mit den europäischen Vorschlägen sollte Deutschland seine Erfahrungen evaluieren und in den europäischen Diskussionsprozess positiv einbringen.

Dies vorangestellt verbleiben wenige Punkte im Verordnungsvorschlag, die aufgrund dieser deutschen Praxiserfahrungen noch besser geregelt werden sollten.

3.1 Bestellungspflicht eines betrieblichen/behördlichen Datenschutzbeauftragten

Die verbindliche europaweite Einführung dieses Konzeptes innerbetrieblicher Selbstkontrolle stellt einen wichtigen Fortschritt zur bisherigen Situation dar. Bei allen berechtigten Zweifeln an der Wirksamkeit schlecht ausgebildeter und ausgestatteter Datenschutzbeauftragter ist deren Wirksamkeit für eine Grundsensibilisierung des bestellenden Unternehmens bzw. der jeweiligen Behörde unbestritten. Diesen Unterschied kann man sehr instruktiv innerhalb Deutschlands bei einem Vergleich behördlicher Datenschutzpraxis zwischen Bundesländern beobachten, die einen behördlichen Datenschutzbeauftragten eingeführt haben und solchen ohne bzw. auf freiwilliger Basis. Insofern wäre die Umsetzung des Vorschlages der Kommission auch für deutsche Behörden ein erheblicher Fortschritt.

Bedauerlicherweise scheint die Kommission einem auch in Deutschland gern verbreitetem Irrtum aufgesessen zu sein und die Bestellungspflicht als eine bürokratische Belastung anzusehen, von der klein- und mittelständische Unternehmen befreit werden müssten (und könnten). Das Gegenteil ist der Fall: diese Unternehmen werden wesentlich mehr finanziellen und organisatorischen Aufwand betreiben müssen, wollten Sie die materiell-rechtlichen Anforderungen vergleichbarer Unternehmen umsetzen. Hier wird oft erst zu spät – also reaktiv – und dann mit dem Schwerpunkt juristischer Schadensabwehr – also durch die Einbeziehung kostenintensiver Rechtsberatung – wesentlich größerer aufwand erzeugt, also durch einen proaktiv wirkenden Datenschutzbeauftragten. Vor dem Hintergrund dieser Feststellung entpuppt sich die vorgesehen Bestellungsgrenze entweder als ein vergiftetes Geschenk oder den heimlichen Versuch, diese Unternehmen mangels effektiver Kontrollmöglichkeiten der Aufsichtsbehörden auch materiell-rechtlich einen Freibrief erteilen zu wollen.

Die vorgesehene Bestellungsgrenze von 250 Mitarbeitern entspringt offensichtlich der Definition von Eurostat für klein- und mittelständische Unternehmen und entlastet somit allenfalls die Statistiker.

Im Sinne der Zielstellung eines wirksamen Grundrechtsschutzes wesentlich wirksamer wäre hingegen eine Definition der Bestellungsgrenze, die an die Art der Datenverarbeitung und damit verbundene Gefahren anknüpft.

Die öffentliche Kritik der Datenschutzverbände richtet sich vor allem gegen Artikel 35 Absatz 1 lit.b EU-DSGVO-E, wonach der für die Verarbeitung Verantwortliche und der

Auftragsverarbeiter einen Datenschutzbeauftragten benennen, falls „die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt“. Hiernach entstünde tatsächlich die ungewöhnliche Konstellation, dass beispielsweise ein großes medizinisches Rechenzentrum mit 100 Mitarbeitern von der Bestellungspflicht entbunden würde, eine Werft mit 1500 Mitarbeitern hingegen, in der lediglich in der Personalabteilung personenbezogene Daten verarbeitet werden, nicht.

Nach Art. 35 Absatz 1 lit. c soll der für die Verarbeitung Verantwortliche einen Datenschutzbeauftragten benennen, falls „die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke **eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.**“

Redaktionelles Versehen?

Bereits der Versuch Fälle zu identifizieren, in denen Verarbeitungsvorgänge „aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke“ eine regelmäßige „Beobachtung von betroffenen Personen erforderlich machen“ könnte, lässt den Interpreten stutzen. Sollte hier wirkliche eine Spezialregelung für Fälle gemeint sein, in denen Protokolldaten erzeugt werden, um Mitarbeiterverhalten zu überwachen? Aber für welche Art von Unternehmen stellt eine solche Datenverarbeitung eine „Kerntätigkeit“ dar? Eine polizeiliche oder geheimdienstliche Tätigkeit kann hier schon nicht gemeint sein, da diese allenfalls durch den ebenfalls vorliegenden Richtlinienvorschlag umfasst würde.

Da liegt es nahe, sich in der Begründung des Verordnungsvorschlages nach einem Hinweis auf die Regelungsabsicht umzuschauen. Dort stößt der Ratsuchende auf folgende Formulierung:

„Artikel 35 schreibt die Einsetzung eines Datenschutzbeauftragten für den öffentlichen Sektor sowie im privaten Sektor für Großunternehmen und in Fällen vor, in denen die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters aus Verarbeitungsvorgängen besteht, **die einer regelmäßigen, systematischen Überwachung bedürfen**. Gestützt ist diese Bestimmung auf Artikel 18 Abs. 2 der Richtlinie 95/46/EG, der den Mitgliedstaaten die Möglichkeit bietet, als Ersatz für die allgemeine Meldepflicht die Bestellung eines Datenschutzbeauftragten vorzusehen“[5]. Hiermit wird deutlich, dass es sich bei der Einfügung des Merkmals „von betroffenen Personen“ nur um ein redaktionelles Versehen handeln kann und die Formulierung richtigerweise lauten muss: „welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung erforderlich machen“.

Zu diesem Ergebnis käme auch eine genauere Betrachtung der Übersetzung, wenn man von der englischen Arbeitsfassung ausgeht. Dort heißt es in der Begründung „which require regular and systematic monitorig", im Gesetzestext dann jedoch „require systematic monitoring of data subjects“. Hier hat sich also wohl ein systematischer Fehler dann auch in der Übersetzung durchgesetzt.

[5] KOM (2012) 11/4, Begründung, Erläuterung des Vorschlag im Einzelnen, 3.4.4.4. Abschnitt 4 – Datenschutzbeauftragter; Hervorhebung durch den Autor

auslegungsbedürftiger Regelungsvorschlag

Damit wäre die Gefahr eines „Generalangriffs auf das deutsche Datenschutzniveau“ jedoch noch nicht gebannt. Es stellt sich weiterhin die Frage, welche Datenverarbeitungsvorgänge denn dann eine regelmäßige und systematische Beobachtung durch einen betrieblichen Datenschutzbeauftragten erforderlich machen sollen. Die Antwort hierauf findet sich ebenfalls bereits im Verordnungsentwurf.

Unstreitig dürfte sein, dass genehmigungspflichtige Verarbeitungen offensichtlich gemeint sein dürften. Nach Artikel 34 Absatz 1 sind Verarbeitungen durch die Aufsichtsbehörde zu genehmigen, wenn der für die Verarbeitung Verantwortliche „Vertragsklauseln nach Artikel 42 Absatz 2 Buchstabe d vereinbart oder keine geeigneten Garantien für die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation in einem rechtsverbindlichen Instrument nach Artikel 42 Absatz 5 vorsieht“.

risikobehaftete Datenverarbeitungsvorgänge

Gemäß Artikel 33 Absatz 1 hat die verantwortliche Stelle aber bereits eine Datenschutz-Folgenabschätzung in den Fällen vorzunehmen, in denen Verarbeitungsvorgänge aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen. Dort werden diese ausführlich weiter konkretisiert:

„Die in Absatz 1 genannten Risiken bestehen insbesondere bei folgenden Verarbeitungsvorgängen:

a) systematische und umfassende Auswertung persönlicher Aspekte einer natürlichen Person, beispielsweise zwecks Analyse ihrer wirtschaftlichen Lage, ihres Aufenthaltsorts, ihres Gesundheitszustands, ihrer persönlichen Vorlieben, ihrer Zuverlässigkeit oder ihres Verhaltens oder zwecks diesbezüglicher Voraussagen, …

b) Verarbeitung von Daten über das Sexualleben, den Gesundheitszustand, die Rasse oder die ethnische Herkunft oder für die Erbringung von Gesundheitsdiensten, für epidemiologische Studien oder für Erhebungen über Geisteskrankheiten oder ansteckende Krankheiten,…;

c) weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels Videoüberwachung;

d) Verarbeitung personenbezogener Daten aus umfangreichen Dateien, die Daten über Kinder, genetische Daten oder biometrische Daten enthalten;

e) sonstige Verarbeitungsvorgänge, bei denen gemäß Artikel 34 Absatz 2 Buchstabe b vorab die Aufsichtsbehörde zu Rate zu ziehen ist.“

Mit der Bezugnahme auf Artikel 34 Absatz 2 lit. b werden alle Fälle umfasst, in denen „die Aufsichtsbehörde eine vorherige Zurateziehung bezüglich der in Absatz 4 genannten Verarbeitungsvorgänge, welche aufgrund ihres Wesens, ihre Umfangs und/oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen können, für erforderlich hält.“ Hier eröffnet Artikel 34 Absatz 4 neben den aus anderen Gründen kritikwürdigen Regelungsbefugnissen der Kommission darüber hinaus eine Auslegungsbefugnis für die Aufsichtsbehörden. „Die Aufsichtsbehörde erstellt eine Liste der

Verarbeitungsvorgänge, die Gegenstand der vorherigen Zurateziehung nach Absatz 2 Buchstabe b sind, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt derartige Listen an den Europäischen Datenschutzausschuss."

überwachungsbedürftige Verarbeitungsvorgänge

So begrüßenswert die Möglichkeit der Aufsichtsbehörden ist, den Katalog in einem einfachen Verfahren um neue Gefährdungsklassen zu erweitern und zu konkretisieren, so könnte und sollte er vom Gesetzgeber noch weiter mit dem Ziel beraten werden, ob hiermit bereits alle Regelfälle besonders risikoreicher Datenverarbeitungen umfasst sind. So könnte die Aufnahme von Verfahren zur Überwachung des Arbeitsverhaltens ebenso hilfreich sein, wie die generelle Aufnahme von Datenverarbeitungsverfahren, die sich an Kinder richten. Es erschließt sich auch nicht, warum einerseits besondere Arten personenbezogener Daten definiert werden, diese dann aber nur bei „umfangreichen" Dateien der Kontrolle eines betrieblichen Datenschutzbeauftragten unterzogen werden sollen. Hier sollte der Grundrechtsschutz nicht an eine bestimmte Menge von Betroffenen geknüpft werden.

Eine solche Liste von überwachungsbedürftigen Verarbeitungsvorgängen würde damit nach der hier vertretenen Auffassung nicht nur das Erfordernis einer internen und externen Vorabkontrolle auslösen, sondern auch die Pflicht zur Bestellung eines Datenschutzbeauftragten als Mittel einer effektiven und qualifizierten, betrieblichen Selbstkontrolle. Diese Lösung wäre auch sachgerecht, fließen so doch qualitativ bestimmbare Gefährdungsaspekte in die Bestellungspflicht für einen Datenschutzbeauftragten ein.

Kerntätigkeit

Die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters ist in der Regel die Erfüllung des Geschäftszwecks und dieser ist nur selten die Datenverarbeitung. Gerade in den Bereichen geschäftsmäßiger Datenverarbeiter ist der Datenschutz zumindest als Datensicherheit verstanden vergleichsweise gut umgesetzt. Eine Reduzierung der typischen Gefährdungen für das Recht auf Datenschutz auf die wenigen – in der Regel kriminellen – kommerziellen Anbieter liefe ohnehin in die Leere wirtschaftlicher Graubereiche. Der Verordnungsvorschlag überlässt die Definition des Kernbereiches in Nummer 11 der Kommission – eine aus vielen Gründen unbefriedigende Situation.

Für diese Einschränkung ist kein vernünftiger Grund ersichtlich. Die großen Gefahren gehen heute von oft kleinen Datenverarbeitungssystemen und den Verschneidungsmöglichkeiten von Datensammlungen aus. Die materiell-rechtlichen Regelungen des Verordnungsvorschlages definieren Anforderungen und Verfahren für jede Datenverarbeitung – unabhängig ob Kerntätigkeit oder nur Dienstleistung oder Infrastruktur.

Zur Klarstellung einer solchen Auslegung des Verordnungsvorschlages wäre es hilfreich, im Rahmen der anstehenden parlamentarischen Beratung den Text wie folgt zu fassen:

Regelungsvorschlag Artikel 35

„Artikel 35 Benennung eines Datenschutzbeauftragten

1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls

a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; oder

b) die **Verarbeitung** durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt, oder

c) **der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter Verarbeitungsvorgänge betreibt**, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke **insbesondere in den Fällen der Artikel 33 und 34** eine regelmäßige und systematische Beobachtung erforderlich machen.“

3.2 Arbeitnehmerdatenschutz

Die Kommission hat es bisher unterlassen, eine eigenständige Vollregelung für den umfangreichen Bereich der Beschäftigtendatenverarbeitungen vorzunehmen. Dabei ist dieser Bereich unternehmerischer Datenverarbeitungen neben der Verarbeitung von Kundendaten in allen Unternehmen anzutreffen und Schwerpunkt der betriebsinternen Überwachungstätigkeit der Datenschutzbeauftragten. Es macht wenig Sinn, diesen insbesondere für grenzüberschreitend tätige Unternehmen wichtigen Bereich automatisierter Datenverarbeitung der nationalstaatlichen Regelung zu überlassen.

Zumindest die wichtigsten Eckpunkte sollten europaweit einheitlich verankert werden, um hier die Freizügigkeit der Arbeitnehmer und den freien Binnenmarkt zu befördern, ohne die Rechte der Arbeitnehmer weiterhin 27 verschiedenen Regelungen zu überlassen.

Regelungsvorschlag Arbeitnehmerdatenschutz

Textvorschlag Artikel 82 DSGVO-E

1.Die Bestimmungen, Grundsätze und Prinzipien dieser Verordnung gelten auch für die Verarbeitung von Beschäftigtendaten durch Arbeitgeber. Personalakten und vergleichbare Personalunterlagen gelten als Datei im Sinne von Art. 4 Abs. 1 Ziffer 4.

2.Beschäftigtendaten dürfen vom Arbeitgeber ausschließlich in einer Weise und für Zwecke verarbeitet werden, die entweder

a.durch ein Gesetz verbindlich vorgeschrieben sind oder

b.für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich sind oder

c.für die Erfüllung arbeitsvertraglicher Pflichten oder die Wahrnehmung von aus dem Beschäftigungsverhältnis resultierenden Rechten erforderlich sind oder

d.für den ordnungsgemäßen Betrieb informationstechnischer Systeme erforderlich sind oder

e.durch ohne Zwang vom Beschäftigten genutzte innerbetriebliche Dienste erforderlich sind.

3.Medizinische Daten von Beschäftigten, insbesondere solcher, die im Rahmen arbeitsmedizinischer Untersuchungen nach Art. 81 Abs. 1 Buchstabe a erhoben wurden, dürfen auch gegenüber dem Arbeitgeber nicht offenbart werden.

4.In den Fällen der Buchstaben b.-e. und im Rahmen dieser Verordnung können nationale Gesetze oder kollektive Vereinbarungen zwischen Arbeitgebern und Arbeitnehmern, soweit diese gesetzlich vorgesehen sind, Zulässigkeitsgrundlagen für konkrete Verfahren, Verfahrensgestaltung oder Umsetzungen schaffen oder

Verarbeitungsverbote aussprechen.

5.Ist in einem Unternehmen nach dem Recht des Mitgliedsstaates eine Vertretung der Beschäftigten eingerichtet, so ist die Verarbeitung durch den Arbeitgeber nur zulässig, wenn die gesetzlich vorgeschriebenen Beteiligungsrechte eingehalten wurden.

6.Ist die Übermittlung von Beschäftigtendaten an Stellen außerhalb des Geltungsbereichs dieser Verordnung beabsichtigt, so ist in jedem Fall eine Prüfung durch den Datenschutzbeauftragten des Arbeitgebers nach Art. 33 vorzunehmen.

7. Unter Verstoß gegen diese Verordnung erhobene oder verarbeitete Daten über das Verhalten oder die Leistung von Beschäftigten dürfen weder gerichtlich noch außergerichtlich verwendet werden.

8.Arbeitnehmervertretungen oder Gewerkschaften können Rechte nach Artikel 76 für die von ihnen vertretenen Beschäftigten wahrnehmen.

3.3 Verfahrensverzeichnis wirksam erhalten

Das in Deutschland als Verfahrensverzeichnis etablierte Verzeichnis aller Datenverarbeitungen hat die Kommission unter Artikel 28 als Dokumentation aufgenommen. Hierbei hat die Kommission es allerdings unterlassen zu regeln, dass diese Dokumentation auf Antrag jedermann zur Einsicht bereit zu halten ist. Damit würde das wirksamste Instrument zur Durchsetzung dieser durchaus aufwändigen Dokumentationspflicht und zugleich eine wirksame externe Kontrollmöglichkeit entfallen. Die Aufsichtsbehörden werden nicht in der Lage sein, dies durch eigene Kontrollen auszugleichen.

Regelungsvorschlag Artikel 28 Nummer 3

3. Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen stellen die Dokumentation der Aufsichtsbehörde **und mit Ausnahme der Angaben nach Buchstabe h jedermann** auf Anforderung **unentgeltlich** zur Verfügung.

---

gez. Karsten Neumann, 19. Oktober 2012