

Werner Hülsmann

Datenschutz in der Pflege

Angesichts des Zuwachses an privaten Einrichtungen für die ambulante und stationäre Pflege sowie der Sensibilität der »Kundendaten« der Pflegeeinrichtungen ist es verwunderlich, dass die Thematik Datenschutz in Pflegeeinrichtungen weder in der Fachliteratur noch in Bildungsangeboten einen angemessenen Niederschlag findet. Dabei sind gerade in Pflegeeinrichtungen unterschiedliche gesetzliche Bestimmungen zum Schutz der Patienten- bzw. Klientendaten¹ aber auch der Mitarbeiterdaten zu berücksichtigen.

Vielen Pflegeeinrichtungen ist allerdings nicht bekannt, dass sie sich um das Thema Datenschutz kümmern müssen und noch viel weniger Einrichtungen wissen, ab wann sie einen Datenschutzbeauftragten bestellen und schulen lassen müssen. Dies gilt für alle Arten von Pflegeeinrichtungen. Im Bereich der Pflege können grob zwei Arten von Einrichtungen unterschieden werden:²

1. Ambulante Pflegedienste: Hier werden die Klienten bei sich Zuhause von den Pflegekräften des ambulanten Pflegedienstes betreut.
2. Stationäre Pflege / Pflegeheim: Die Klienten leben im Pflegeheim.

In der Praxis gibt es noch weitere Ausprägungen, wie beispielsweise die Tagespflege (»teilstationäre Pflege«³), hier halten sich Klienten nur tagsüber in der stationären Pflegeeinrichtung auf, oder das betreute Wohnen. Die meisten datenschutzrechtlichen Grundlagen gelten gleichermaßen für ambulante wie für stationäre Pflegeeinrichtungen. Wie Tabelle 1 zeigt, werden in Pflegeeinrichtungen – gerade auch von den Klienten – sehr sensible Daten verarbeitet.

Die Einhaltung des Datenschutzes

¹ Im Bereich der Pflege wird je nach Einrichtung von Patienten, Klienten oder auch von Kunden gesprochen. Im Folgenden wird der Einfachheit halber der Begriff »Klienten« – unabhängig von der Einrichtungsart – verwendet.

² Vgl. § 71 SGB XI.

³ Vgl. § 41 SGB XI.

ist allerdings nicht nur eine gesetzliche Verpflichtung, sondern ist auch eine wichtige Voraussetzung für das Vertrauen der Klienten in die Pflegeeinrichtung. Der sorgfältige Umgang mit Klientenunterlagen ist bei vielen Einrichtungen eine Selbstverständlichkeit. Allerdings bringt die zunehmende Nutzung der EDV, die auch in den Pflegeeinrichtungen nicht mehr wegzudenken ist, immer stärker die Gefahr mit sich, dass durch Unachtsamkeit, fehlendes Risikobewusstsein oder technische Unzulänglichkeiten die Vertraulichkeit der anvertrauten Klientendaten nicht mehr gewährleistet ist. Hier ist neben den betrieblichen Datenschutzbeauftragten – sofern diese vorhanden sind – die Pflegedienstleitung gefordert, die erforderlichen Maßnahmen zur Sensibilisierung der Mitarbeiter/innen und zum Schutz der Daten und Unterlagen zu ergreifen.

Kontrolle des Datenschutzes

Neben der Kontrolle durch die zuständigen Datenschutzaufsichtsbehörden und den betrieblichen Datenschutzbeauftragten werden bei den Pflegeein-

richtungen auch im Rahmen der Qualitätsprüfungen durch den Medizinischen Dienst der Krankenkassen (MDK) bzw. der Heimaufsicht zumindest Teilaspekte der Umsetzung des Datenschutzes in der Pflegeeinrichtung abgefragt. So wird beispielsweise im Fragenkomplex zur räumlichen Ausstattung bei ambulanter Pflege (Frage 2.1) danach gefragt, ob personenbezogene Unterlagen für Unbefugte unzugänglich aufbewahrt werden. Im Fragenkomplex 3 zur Aufbauorganisation Personal wird sowohl bei ambulanten als auch stationären Pflegeeinrichtungen nach einer verbindlichen Regelung der Verantwortungsbereiche gefragt, die auch aus Sicht des Datenschutzes erforderlich ist. Nur bei klarer Regelung der Verantwortungsbereiche lässt sich die zur Sicherstellung des Datenschutzes wichtige Frage beantworten, wer auf welche personenbezogenen Daten Zugriff haben darf und muss. Weitere datenschutzrelevante Fragestellungen aus den Erhebungsbögen für ambulante und stationäre Pflegeeinrichtungen sind die Frage nach der Dokumentenechtheit der Dienstpläne (Frage 4.4), die Frage nach der Pflegedokumentation (Fragen 7.1 und 7.2) und die Anforderungen an eine computergestützte Pfl-

Tab. 1: Beispiele für personenbezogene Daten in Pflegeeinrichtungen

Betroffene	Personenbezogene Daten der Betroffenen
Klienten	Name, Anschrift, Sozialversicherungsnummer, Krankenkasse, Pflegestufe, Pflegedokumentation, Religion, Namen und Anschrift von Angehörigen, ...
Angehörige der Patienten/Klienten	Name, Anschrift, Telefonnummer, Verwandtschaftsverhältnis zum Patienten/Klienten, ...
Mitarbeiter	Name, Anschrift, Telefonnummer, Sozialversicherungsnummer, Bankverbindung, Gehalt, Steuerklasse, Kirchensteuerabzug, Freibeträge, Krankenkasse, Qualifikation, Daten aus der Pflegedokumentation, Daten aus der Schichtplanung, KFZ-Kennzeichen des Dienstfahrzeugs, Fahrtenbuch, ...
Lieferanten, Dienstleister	Name, Anschrift, Telefonnummer, Ansprechpartner, E-Mail-Adresse, Lieferkonditionen, Rechnungsdaten, ...

gedokumentation (Frage 7.3). Darüber hinaus wird immer stärker auch zumindest die Umsetzung des Klientendatenschutzes im Rahmen der Zertifizierung der Qualitätssicherungsmaßnahmen berücksichtigt.

Datenschutzrechtliche Anforderungen in Pflegeeinrichtungen

Jede Pflegeeinrichtung arbeitet mit Klienten- und Mitarbeiterdaten. Selbst kleinere Einrichtungen kommen an der Nutzung von PCs nicht mehr vorbei. Der Umgang mit diesen teilweise sehr sensiblen, elektronisch gespeicherten Informationen ist nicht nur durch das Bundesdatenschutzgesetz (BDSG), sondern durch weitere bereichsspezifische Datenschutzvorschriften geregelt. Wie in vielen anderen Branchen ist allerdings auch im Pflegebereich die Auffassung weit verbreitet, dass nur große Einrichtungen sich um den Datenschutz kümmern müssen. Der Irrglaube, dass nur Einrichtungen und Firmen, die einen Datenschutzbeauftragten bestellen müssen, sich auch um den Datenschutz kümmern müssen, ist auch durch die 2006 mit der Einfügung von Absatz 2a im § 4g BDSG⁴ erfolgten Klarstellung des Gesetzgebers leider nicht ausgestorben.

Eigentlich sollte es eine Selbstverständlichkeit sein: Bei der Umsetzung der Maßnahmen zum Datenschutz ist die besondere Sensibilität der Klientendaten zu berücksichtigen. In der Praxis finden sich oftmals aber Systeme sowie technische und organisatorische Maßnahmen, die für die Kundendatenverarbeitung eines »normalen« Dienstleistungsunternehmens als ausreichend angesehen werden können. Gerade beim Outsourcing von Dienstleistungen, sei es die Installation und Wartung der EDV, sei es die Abrechnung mit den Kranken- bzw. Pflegekassen, werden die besonderen Anforderungen, die sich aus Patienten- und Sozialgeheimnis ergeben, vielfach nicht in ausreichender Weise berücksichtigt.

⁴ »Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.« (§ 4g Abs. 2a BDSG).

Das Patienten- und das Sozialgeheimnis

Die Klientendaten unterliegen nicht nur dem Datenschutz, sondern – auch wenn sie nicht automatisiert verarbeitet werden – dem Patientengeheimnis aus dem § 203 Abs. 1 StGB. Danach wird mit Freiheitsstrafe bis zu einem Jahr bestraft, wer als Krankenschwester oder -pfleger (aber auch als Arzt/Ärztin oder Heilpraktiker/in) unbefugt Privatgeheimnisse der Patient/inn/en offenbart.

Pflegeeinrichtungen, die – wie es meist der Fall ist – als Leistungserbringer der Kranken- oder Pflegeversicherung tätig sind, unterliegen bezüglich der in diesen Zusammenhang stehenden Klientendaten dem Sozialgeheimnis aus § 35 SGB I und müssen die Anforderungen des Sozialdatenschutzes berücksichtigen. Im Geltungsbereich des Sozialgeheimnisses und des Sozialdatenschutzes ist zu beachten, dass auch die Daten von Verstorbenen dem Sozialgeheimnis und dem Sozialdatenschutz unterliegen und auch Betriebs- und Geschäftsgeheimnisse den Sozialdaten gleichgestellt sind.

Anwendbare gesetzliche Regelungen

Neben dem Patienten- und Sozialgeheimnis sind die folgenden rechtlichen Regelungen im Bereich der Pflege anwendbar.

- Elftes Buch Sozialgesetzbuch (SGB XI), insbesondere das neunte Kapitel »Datenschutz und Statistik« mit Verweis auf § 35 des Ersten Buches (SGB I) sowie die §§ 67 bis 85 des Zehnten Buches (SGB X). Der dritte Abschnitt von Kapitel 9 SGB XI regelt die Rechte und Pflichten der Leistungserbringer – das sind die von den Pflegekassen anerkannten Pflegeeinrichtungen.
- Heimgesetz (HeimG), § 13 regelt für stationäre Einrichtungen Aufzeichnungs- und Aufbewahrungsfristen.
- Strafgesetzbuch (StGB), neben dem Patientengeheimnis (§ 203 StGB) finden sich hier Regelungen zum rechtfertigten Notstand (§ 34 StGB), zur Nichtanzeige von Straftaten und der Strafflosigkeit der Nichtanzeige geplanter Straftaten (§§ 138, 139 StGB).
- Bürgerliches Gesetzbuch (BGB), Regelungen zur Nichtigkeit wegen Formmangels (z.B. von Einwilligungsförmularen) und der elektronischen Form (§§ 125, 126a BGB), Nichtigkeit gesetzwidriger Rechtsgeschäfte (§ 134 BGB) sowie

Regelungen zu Vollmachten (§§ 167 ff BGB) und Regelungen zu Rechtsgeschäften, bei denen eine Zustimmung durch Dritte erforderlich ist (§§ 182f BGB).

- Strafprozessordnung (StPO) und Zivilprozessordnung (ZPO), Regelungen zum Zeugnisverweigerungsrecht (§ 53 StPO bzw. § 383 ZPO).

Daneben sind die üblichen bereichsspezifischen Regelungen zu berücksichtigen, die für alle Unternehmen einschlägig sind, wie z.B. die Abgabenordnung bezüglich der Lohn- und Kirchensteuerabzüge, das Telemediengesetz für die eigene Website, etc. Und – last but not least – gilt das Bundesdatenschutzgesetz dann, wenn keines der vorgenannten Gesetze bereichsspezifische Regelungen enthält.

Datenschutzrechtliche Verpflichtungen aller Pflegeeinrichtungen

Wie alle Unternehmen und Institutionen sind auch Pflegeeinrichtungen unabhängig von der Anzahl der Mitarbeiter verpflichtet, die datenschutzrechtlichen Anforderungen umzusetzen. Hierzu gehören nach BDSG § 9 bzw. SGBX § 78a die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit, die Erstellung von Verfahrensbeschreibungen, die Verpflichtung der Mitarbeiter auf das Daten-, Patienten- und Sozialgeheimnis, die Benachrichtigung der Betroffenen über die erstmalige Speicherung personenbezogener Daten (sofern keine der Ausnahmen anwendbar ist), das Berichten, Sperren oder Löschen der personenbezogenen Daten von Betroffenen, wenn die Daten nicht mehr benötigt werden bzw. unzulässigerweise verarbeitet wurden, sowie die Auskunft über gespeicherte Daten an die Betroffenen.

Bestellung eines Datenschutzbeauftragten

Wenn mehr als neun Personen in der Regel personenbezogene Daten automatisiert verarbeiten, also EDV-gestützt erheben, verarbeiten oder nutzen, ist die Pflegeeinrichtung – wie alle anderen Unternehmen auch – nach § 4f BDSG verpflichtet einen betrieblichen Datenschutzbeauftragten zu bestellen. Hier kommt es nicht auf die Anzahl der Arbeitsplätze, sondern auf die Anzahl

der Personen an – unabhängig von ihrer Arbeitszeit. Teilen sich z.B. zwei Mitarbeiter einen Arbeitsplatz am PC, dann sind beide Mitarbeiter mitzuzählen. Zu den Personen, die mitzuzählen sind, gehören nicht nur Arbeitnehmer, sondern – seit der BDSG-Novellierung 2006 – auch Auszubildende und Praktikanten sowie Inhaber, sofern diese in der Regel auch mit der automatisierten Datenverarbeitung beschäftigt sind.

Ein Datenschutzbeauftragte ist auch dann zu bestellen, wenn automatisierte Verarbeitungen personenbezogener Daten vorgenommen werden, die der Vorabkontrolle unterliegen (vgl. § 4d Abs. 5, 6 BDSG) oder mindestens 20 Personen personenbezogene Daten verarbeiten, auch wenn dies ohne Computerunterstützung geschieht.

Wer kann zum betrieblichen Datenschutzbeauftragten bestellt werden?

Der betriebliche Datenschutzbeauftragte muss die notwendige Fachkunde und Zuverlässigkeit für eine ordnungsgemäße Aufgabenerfüllung besitzen. Darüber hinaus muss die Leitung der Einrichtung ihm auch die erforderliche Zeit und die Mittel für Aufgabenerfüllung und Fort- und Weiterbildung zur Verfügung stellen. Die Tätigkeit des Datenschutzbeauftragten kann von einem bereits in der Pflegeeinrichtung beschäftigten Mitarbeiter zusätzlich übernommen werden. Dabei ist darauf zu achten, dass dem Datenschutzbeauftragten genügend Zeit für diese Aufgabe zugestanden wird und er im Bereich seiner sonstigen Aufgaben zeitlich entlastet wird. Insbesondere zu Beginn der Tätigkeit darf der Aufwand nicht unterschätzt werden. Schließlich benötigt der neue Datenschutzbeauftragte zur Erlangung der erforderlichen Fachkunde eine ausreichende Fortbildung und hat auch noch keine Routine bei der Umsetzung entwickelt. Zudem gibt es viele Tätigkeiten, die am Anfang mit einem einmaligen höheren Aufwand verbunden sind, wie das Erstellen der Verfahrensbeschreibungen, die Einführung eines Datenschutzmanagements oder die Unterweisung der Mitarbeiter im Datenschutz an ihrem konkreten Arbeitsplatz.

Zuverlässigkeit

Zum einen ist die persönliche Zuverlässigkeit gefordert. Dies heißt, dass

der ausgewählte Mitarbeiter seine Aufgaben als Datenschutzbeauftragter verantwortlich erfüllt und die Verschwiegenheitsverpflichtungen als Datenschutzbeauftragter einhält. Zum anderen ist die fachliche Zuverlässigkeit gefordert. Bei der Auswahl des Mitarbeiters, der zum Datenschutzbeauftragten bestellt werden soll, ist – zur Sicherstellung dieser fachlichen Zuverlässigkeit – darauf zu achten, dass es beim Mitarbeiter nicht zu Interessenkollisionen zwischen der Tätigkeit als Datenschutzbeauftragten und der sonstigen Tätigkeit kommt. Daher sind grundsätzlich IT-/EDV- oder Personalverantwortliche ebenso wenig wie die Pflegedienstleistung für diese Tätigkeit geeignet. Da der Datenschutzbeauftragte direkt der Leitung der Stelle unterstellt werden muss, kann auch die Geschäftsführung oder der Vorstand der Einrichtung die Tätigkeit des Datenschutzbeauftragten nicht selbst übernehmen.

Fachkunde

Zur erforderlichen Fachkunde gehört nicht nur, dass der Datenschutzbeauftragte weiß, welche Regelungen des BDSG für seine Einrichtungen gelten und wie diese anzuwenden sind, sondern auch, welche bereichsspezifischen Regelungen gelten (s.o.) und wie diese umzusetzen sind.

Zu den organisatorischen Qualifikationsanforderungen an betriebliche Datenschutzbeauftragte gehören:

- Eigenverantwortliche und selbstorganisierte Aufgabenerledigung. Dies gilt umso mehr, da die Tätigkeit als Datenschutzbeauftragter meist nur neben der »normalen« Tätigkeit ausgeführt werden kann.
- Effizientes Zeitmanagement.
- Eine gewisse Durchsetzungskraft und Konfliktbereitschaft, verbunden mit Dialogbereitschaft.
- Die Fähigkeit, komplexe Sachverhalte einfach darstellen zu können.

Fortbildung für angehende Datenschutzbeauftragte

Der für die Tätigkeit zum Datenschutzbeauftragten ausgewählte Mitarbeiter muss die erforderliche Fachkunde in Sachen Datenschutz haben. Daher sollte der angehende Datenschutzbeauftragte in geeigneten Seminaren die erforderliche Ausbildung zum Datenschutzbeauftragten erhalten. Auf der

Website des virtuellen Datenschutzzentrums (www.datenschutz.de/partner/kooperationspartner/) finden sich in der Rubrik »Veranstaltungsanbieter im Bereich Datenschutz und Datensicherheit« Seminaranbieter, die teilweise auch spezielle Angebote zum Datenschutz im Gesundheitswesen in ihrem Programm haben. Bei der Auswahl und Zusammenstellung der Seminare sollte beachtet werden, dass für Datenschutzbeauftragte in Pflegeeinrichtungen allgemeine datenschutzrechtliche Kenntnisse nicht ausreichen, sondern gerade auch Kenntnisse im Sozial- und Gesundheitsdatenschutz erforderlich sind.

Externe Datenschutzbeauftragte

Es besteht auch die Möglichkeit, einen externen Dienstleister mit der Aufgabe des Datenschutzbeauftragten zu betrauen. Im BDSG ist diese Möglichkeit ausdrücklich vorgesehen. Diese Möglichkeit kommt insbesondere dann in Betracht, wenn kein für diese Tätigkeit geeigneter Mitarbeiter in der Pflegeeinrichtung tätig ist und/oder der Aufwand für die erstmalige Aus- und regelmäßige Fortbildung in keinem sinnvollen Verhältnis zum tatsächlichen Aufwand der Tätigkeit in der Pflegeeinrichtung steht. Bei kleineren Pflegeeinrichtungen, die den Schwellenwert zur Bestellung gerade überschreiten, wird letzteres der Fall sein. Ein weiteres Argument für die Bestellung eines externen Datenschutzbeauftragten ist, dass ein erfahrener externer Dienstleister eine gewisse Routine bei der Erledigung der Aufgaben mitbringt und damit für eine effiziente und praxisbezogene Umsetzung des Datenschutzes sorgen kann. Bei der Beauftragung eines externen Dienstleisters muss aber beachtet werden, dass es nicht die gleiche Person sein darf, die eventuell schon die EDV für die Pflegeeinrichtung betreut. Zudem muss die Leitung der Pflegeeinrichtung darauf achten, dass der externe Dienstleister die erforderliche Fachkunde mitbringt und sich nachweislich insbesondere mit Patientendatenschutz und dem Sozialdatenschutz auskennt. Eine sorgfältige Auswahl des Dienstleisters – unter besonderer Berücksichtigung der Qualifikation im Bereich des Sozialdatenschutzes und der Erfahrungen im Pflegebereich – ist daher unerlässlich. Bei einer externen Beauftragung empfiehlt es sich, dass die Einrichtung durch die Benennung eines internen »Datenschutzko-

dinators« die Anbindung des externen Dienstleisters und die fachkundige Umsetzung in der Einrichtung sicher stellt.

Wenn kein Datenschutzbeauftragter zu bestellen ist

»Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.« (§ 4g Abs. 2a BDSG).

Auch ohne diese vom Gesetzgeber 2006 in das BDSG eingefügte Klarstellung war zumindest in Fachkreisen klar, dass jedes Unternehmen – unabhängig von der Größe – die gesetzlichen Verpflichtungen des Datenschutzes erfüllen muss. Durch diese Formulierung wird nun jedem deutlich, dass, wenn kein Datenschutzbeauftragter zu bestellen ist, die Leitung der Einrich-

tung persönlich dafür verantwortlich ist, dass die Aufgaben, die sonst dem Datenschutzbeauftragten obliegen würden, im Unternehmen, in der Pflegeeinrichtung erledigt werden. Dies kann auf unterschiedliche Art und Weise geschehen:

- Die Leitung der Pflegeeinrichtung nimmt die Aufgaben selbst wahr.
- Die Leitung der Pflegeeinrichtung bestellt – obwohl sie nicht dazu verpflichtet wäre – einen betrieblichen Datenschutzbeauftragten.
- Die Leitung der Pflegeeinrichtung delegiert die Aufgaben, die ein betriebliche Datenschutzbeauftragter zu erledigen hätte, an einen oder mehrere Mitarbeiter, deren Verantwortlichkeiten in Bezug auf diese Aufgaben klar geregelt sind.

Auch hier sollte es selbstverständlich sein, dass sich der freiwillig bestellte Datenschutzbeauftragte bzw. der mit den Aufgaben eines Datenschutzbeauftragten beauftragte Mitarbeiter durch Teilnahme an entsprechenden Seminaren mit den datenschutzrechtlichen An-

forderungen und deren praktischen Umsetzungsmöglichkeiten vertraut machen kann.

Fazit

Die Umsetzung der datenschutzrechtlichen Anforderung stellt auch im Bereich der Pflege keine unüberwindbaren Probleme dar und ist – bei entsprechender Bereitschaft der Leitung – auch für kleinere und mittlere Pflegedienste zu meistern, sei es durch entsprechende Fortbildung interner Mitarbeiter oder durch die Beauftragung eines externen Dienstleisters. Eine Unterstützung der Umsetzung des Datenschutzes in Pflegeeinrichtungen durch die Berufsverbände – beispielsweise mit Beratungsangeboten oder durch die Organisation von Fachseminaren sowie die Bereitstellung von konkreten Arbeitshilfen und Materialien für den Pflegebereich – fehlt bisher. Hier besteht noch ein großer Handlungsbedarf.

Umfrage

Kein Rückhalt für Schäubles Anti-Terrorpläne

Laut einer Umfrage des Stern im Juli 2007 befürchteten 54% der BundesbürgerInnen, dass Bundesinnenminister Wolfgang Schäuble einen Überwachungsstaat schafft. Die Gefragten beurteilten die Arbeit des CDU-Politikers, der wegen seiner umstrittenen Vorschläge zur Terrorismusbekämpfung in die öffentliche Kritik geraten ist, durchschnittlich mit der Schulnote 3,3. 41% bewerteten die bisherige Arbeit des Ministers als »befriedigend«; 14% gaben die Note »gut«, nur 2% ein »sehr gut«. Knapp ein Drittel zeigte sich unzufrieden, 21% benoteten mit einem »ausreichend«, 7% mit einem »mangelhaft« und 4% mit einem »ungenügend«.

Für die Umfrage hat das Forsa-Institut am 12. und 13.07.2007 insgesamt 1004 Personen befragt. Dies ist nach Ansicht der Meinungsforschenden repräsentativ für die Bevölkerung mit einer statistischen Fehlertoleranz von 3% nach beiden Seiten. Nach ihrer Einschätzung von Schäuble befragt, hielten ihn von den Befragten 71% für fleißig, 55% für kompetent, nur 40% für ehrlich, 38% für besonnen, 30% für sympathisch und lediglich 17% nannten ihn einen modernen Politiker.

Nach einem ZDF-Politbarometer vom 20.07.2007 erklärten nur 33%, dass die Überlegungen zur Terrorbekämpfung und zum Umgang mit »Gefährdern« richtig seien. Für 45%

gehen die Vorschläge zu weit, für 6% allerdings noch nicht weit genug. 16% hatten keine Meinung zum Thema. Im Juli 2007 rutschte Schäuble mit seinen politischen Forderungen gegenüber Juni in einer Gesamtschau von 0,5 auf 0,2 ab.

Ein Monat zuvor eruierte das Forschungsinstitut Forsa im Auftrag des Stern die Meinung der BürgerInnen zu spezifischen Sicherheitsmaßnahmen. Gefragt wurde, welche Sicherheitsmaßnahmen als unzulässige Eingriffe in die Freiheitsrechte empfunden würden. Danach hielten für unzulässig

- 18% die Videoüberwachung von Bahnhöfen und öffentlichen Plätzen,
- 32% eine zentrale Fingerabdruckdatei,
- 35% einen Zugriff auf Daten aus der LKW-Mautkontrolle,
- 44% die Entnahme von Geruchsproben bei Tatverdächtigen,
- 54% eine sechsmonatige Speicherung aller Verbindungsdaten,
- 59% eine Online-Durchsuchung von Computern,
- 76% das Öffnen von Briefen

(Kreml www.heise.de 18.07.2007 u. 20.07.2007; www.daten-speicherung.de).