



POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1456, 53104 Bonn

Vorsitzender des Innenausschusses
des Deutschen Bundestages
Herrn Wolfgang
Platz der Republik
11011 Berlin

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBUNDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

(0228) 997799-100
(0228) 997799-550
ref5@bfi.bund.de

www.datenschutz.bund.de

Bonn, 14.08.2012

BETREFF **Quellen-Telekommunikationsüberwachung durch die Sicherheitsbehörden**
BEZUG Mein Bericht vom 31.01.2012

Sehr geehrter Herr Vorsitzender,

mit Schreiben vom 31.01.2012 habe ich dem Innenausschuss des Deutschen Bundestages auf dessen Anforderung gemäß § 26 Abs. 2 des Bundesdatenschutzgesetzes meinen Bericht über die Ergebnisse meiner Beratungs- und Kontrollbesuche bei Bundeskriminalamt, Bundespolizei und Zollkriminalamt zugeleitet. Darin hatte ich angekündigt, ergänzende Untersuchungen vorzunehmen und hierüber zu berichten. Im Hinblick darauf möchte ich Ihnen heute folgendes mitteilen:

1. Die Stellungnahmen des Bundesministeriums des Innern und des Bundesministeriums der Finanzen zu den im Bericht vom 31.01.2012 dargestellten Ergebnissen liegen vor.

Beide Ministerien vertreten die Auffassung, die Quellen-Telekommunikationsüberwachung sei durch die geltenden Rechtsgrundlagen gedeckt, zeigen sich für weitere Gespräche im Hinblick auf die Gestaltung einer künftigen Software und einer künftigen standardisierten Leistungsbeschreibung offen und betonen die Ein-



richtung eines „Kompetenzzentrums Informationstechnische Überwachung (CC ITÜ)“. Zur Standardisierten Leistungsbeschreibung werde ich derzeit beteiligt.

Das BMF erkennt die Kritik an der Verschlüsselung und an den Löschungsmöglichkeiten für Inhalte aus dem Kernbereich privater Lebensgestaltung weitgehend an. In einzelnen Bereichen erläutert bzw. präzisiert es einzelne Feststellungen. Es betont, dass bereits vor meinem Besuch im ZKA in Auftrag gegeben worden war, die Software im Hinblick auf die Löschung kernbereichsrelevanter Inhalte anzupassen. Soweit anfänglich in einem Fall eine Software der Firma ERA genutzt worden sei, habe das ZKA lediglich die Markterkundung betrieben sowie handelsübliche Hardware beigelegt. Für die Quellen-TKÜ-Maßnahmen, die mit ERA durchgeführt wurden, sei die Auswahl, Vertragsabwicklung und Beschaffung durch die jeweils ermittelnde Behörde ohne Beteiligung des ZKA erfolgt.

Das BMI hält das eingesetzte Verschlüsselungsverfahren für ausreichend im Sinne des § 9 BDSG, sieht allerdings Optimierungsbedarf. Einen Verstoß gegen die Pflicht, Inhalte aus dem Kernbereich privater Lebensgestaltung zu löschen, sieht das BMI nicht in dem Fehlen einer Funktion zur abschnittsweisen Löschung kernbereichsrelevanter Inhalte. Dies bedeute lediglich, dass im Zweifel mehr Inhalte gelöscht werden müssten. BMI sieht damit insgesamt zwar Verbesserungspotentiale, aber keinen rechtlichen Handlungsbedarf. Das BMI betont darüber hinaus, dass keine Verpflichtung bestanden habe, den Quellcode zur Dokumentation der Datensicherheit zur Verfügung zu halten.

Zu den Ausführungen des BMI merke ich an, dass ich an meinen im Prüfbericht festgestellten Positionen festhalte.

Nach wie vor erachte ich die bisherige Funktion zur Löschung kernbereichsrelevanter Inhalte für unzureichend. So können die unzureichenden Defferenzierungsmöglichkeiten hinsichtlich der zu löschenden Inhalte dazu führen, dass vorsorglich bestimmte, zur Wahrung des Kernbereichsschutzes zu löschende Inhalte weiterhin vorgehalten werden. Andererseits könnte auch dann, wenn diese Funktion dazu führt, dass ggf. „zuviel“ Daten gelöscht werden, dies – etwa im Falle entlastender Beweise – Nachteile für den Betroffenen zur Folge haben.

Ich halte an meiner Position fest, dass § 9 BDSG in verfassungskonformer Auslegung die Dokumentation des Quellcodes bei Maßnahmen der Quellen-Telekommunikationsüberwachung fordert. Diese Maßnahmen sind nicht mit anderen (auch sensiblen) IT-Systemen vergleichbar, über die die verantwortlichen Stellen eine vollständige Kontrolle ausüben. Die mittels Quellen-TKÜ-Software gesteuerten IT-Systeme befinden sich eben nicht ausschließlich im Herrschaftsbe-



reich des Bundeskriminalamts als verantwortliche Stelle. Vielmehr greift das Überwachungssystem insgesamt in die Vertraulichkeit und Integrität informationstechnischer Systeme im Bereich des Betroffenen ein; die Funktionalität der dabei verwendeten Software wird in derartigen Fällen ganz wesentlich davon abhängen, welche auf dem Zielsystem vorhandenen Ressourcen angesteuert bzw. genutzt werden (können). Für derartige Eingriffe hat das Bundesverfassungsgericht besondere Maßnahmen der Datensicherheit gefordert. Es hat die mit der Infiltration des Zielsystems verbundene Gefährdungslage hervorgehoben, aus der besondere Anforderungen an die Datensicherheit und damit auch an die Revisionsicherheit und Dokumentation folgen. Auf meine Ausführungen im Prüfbericht nehme ich Bezug.

2. In meinem Prüfbericht hatte ich meine Absicht angekündigt, den Quellcode der Software einzusehen. Diese Absicht kann ich nicht umsetzen, da ich keinen Zugang zum Quellcode der Software erreichen konnte. Dieser liegt den Ermittlungsbehörden nicht vor. Der Hersteller macht den Zugang von vertraglichen Abreden abhängig, die ich nicht akzeptieren kann. Die datenschutzrechtlichen Vorschriften für meine Kontrollkompetenz sind abschließend. Deshalb ist für etwaige Kostenerstattungsansprüche oder Geheimhaltungsabreden kein Raum.

Bereits während des ersten Beratungs- und Kontrollbesuchs im Bundeskriminalamt wurde mir mitgeteilt, dass der Quellcode der Software dort nicht vorliegt. Meine Mitarbeiter können den Quellcode daher faktisch nur einsehen, wenn die Firma DigiTask GmbH ihn vorlegt. Das Bundeskriminalamt hat sich auf meine Bitte hin bemüht, die Einsichtnahme in den Quellcode zu ermöglichen. Es teilte mir jedoch mit, dass die Firma DigiTask GmbH die Einsichtnahme in den Quellcode nur unter der Voraussetzung ermöglichen werde, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit eine Geheimhaltungsvereinbarung unterzeichne. Darüber hinaus werde die Firma zum Ausgleich der entstehenden Kosten Ansprüche auf Kostenerstattung geltend machen. Der Tagessatz für „Consulting-Dienstleistungen“ betrage 1.200,00 EUR pro Tag und Mitarbeiter zuzüglich der gesetzlichen Mehrwertsteuer. Das Bundeskriminalamt sieht sich nicht zur Tragung dieser Kosten verpflichtet, man werde sich allenfalls anteilig beteiligen. Die von mir vorgeschlagenen Termine waren seitens der DigiTask GmbH nicht realisierbar.

Die datenschutzrechtliche Beratung und Kontrolle führe ich allein auf Grundlage meiner gesetzlichen Aufgaben und Befugnisse nach § 24 Abs. 1 und Abs. 2 BDSG durch. Gegenstand der Kontrolle ist die Erhebung und Verwendung personenbezogener Daten durch Bundesbehörden. Vorliegend geht es um die datenschutzrechtliche Kontrolle, ob und inwieweit bei den Quellen-Telekommunikationsüberwachungsmaßnahmen durch technische Maßnahmen sichergestellt war, dass



ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wurde (insb. § 24 Abs. 1 BDSG i. V. m. § 20I Abs. 2 Nr. 1 BKA-Gesetz). Dies ist letztlich nur mit Hilfe des Quellcodes (der in jedem Einzelfall verwendeten Überwachungssoftware) möglich.

Die Firma DigiTask GmbH ist für meine Behörde weder Vertragspartner noch unterliegt sie meiner datenschutzrechtlichen Kontrolle. Meine datenschutzrechtliche Kontrolle beschränkt sich insoweit auf die öffentlichen Stellen des Bundes.

Kann der Quellcode nicht vom Bundeskriminalamt für Zwecke der Datenschutzkontrolle zur Verfügung gestellt werden, auch nicht auf dessen Veranlassung von einer anderen Stelle, endet meine datenschutzrechtliche Kontrollmöglichkeit. Meine Zuständigkeiten lassen sich auch nicht durch Abreden mit der Firma DigiTask erweitern. Der Bundesbeauftragte handelt insbesondere nicht auf vertraglicher Basis, sondern als öffentliche Kontrollinstanz in gesetzlichem Auftrag

Insbesondere kann meine Prüfungscompetenz nur aufgrund gesetzlicher Grundlage eingeschränkt werden. Eine vertragliche Geheimhaltungsvereinbarung würde meine gesetzlichen Berichtspflichten aus § 26 BDSG beeinträchtigen, wäre also contra legem. Abgesehen davon sind meine Mitarbeiter ohnehin gesetzlich zur Verschwiegenheit verpflichtet, weshalb eine solche Vereinbarung nicht erforderlich ist.

Daher bleibt mir lediglich festzustellen, dass der Quellcode nicht dokumentiert ist und vom BKA für eine datenschutzrechtliche Kontrolle nicht bereitgestellt werden kann. Zwar ist anzuerkennen, dass sich das Bundeskriminalamt aktuell bemüht hat, den Hersteller hierzu zu bewegen. Letztlich hätte dies aber bereits bei der Bestellung der Software in den Verträgen mit dem Hersteller geregelt werden müssen, und zwar nicht nur im Hinblick auf die Gewährleistung der externen Datenschutzkontrolle durch den BfDI, sondern auch, damit das BKA seinen Obliegenheiten als verantwortliche Stelle hätte nachkommen können.

Daher ist es mir im Ergebnis nicht möglich, den Quellcode zur datenschutzrechtlichen Kontrolle zu sichten.

3. Damit ist die datenschutzrechtliche Kontrolle der Quellen-Telekommunikationsüberwachung durch Ermittlungsbehörden des Bundes abgeschlossen.

Teilweise sind die mit der Quellen-Telekommunikationsüberwachung erhobenen personenbezogenen Daten löschungsreif. Auf meine Bitte haben die betroffenen



SEITE 5 VON 5

Behörden von der Löschung dieser Daten abgesehen und diese für Zwecke der datenschutzrechtlichen Kontrolle lediglich gesperrt.

Im Hinblick auf etwaige Nachfragen des Innenausschusses habe ich den betroffenen Behörden noch nicht mitgeteilt, dass die gesperrten Daten endgültig gelöscht werden können. Da es sich um besonders sensible Daten handelt, wäre ich dem Innenausschuss für eine kurzfristige Mitteilung dankbar, ob von dort Bedarf für weitere datenschutzrechtliche Nachfragen oder Nachforschungen gesehen wird.

Mit freundlichen Grüßen