Deutscher Bundestag
16. Wahlperiode

16. Wahlperiode
21. 04. 2009

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 21. April 2009
gemäß § 26 Absatz 1 des Bundesdatenschutzgesetzes.

Unterrichtung
durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Tätigkeitsbericht 2007 und 2008 des Bundesbeauftragten für den Datenschutz und
die Informationsfreiheit
– 22. Tätigkeitsbericht –

Inhaltsverzeichnis

<table>
<thead>
<tr>
<th>Teil</th>
<th>Thema</th>
<th>Seite</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Zur Lage des Datenschutzes in Deutschland</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>Datenschutzrechtlicher Rahmen</td>
<td>18</td>
</tr>
<tr>
<td>2.1</td>
<td>Weiterentwicklung des Datenschutzrechts</td>
<td>18</td>
</tr>
<tr>
<td>2.2</td>
<td>Der „Datenschutzgipfel“ und seine Folgen</td>
<td>20</td>
</tr>
<tr>
<td>2.3</td>
<td>Datenschutz in der Privatwirtschaft – zwei Gesetzesnovellen sollen die Rechte der Betroffenen stärken</td>
<td>21</td>
</tr>
<tr>
<td>2.4</td>
<td>Neuer Anlauf für ein bundesweites Datenschutzaudit</td>
<td>24</td>
</tr>
<tr>
<td>2.5</td>
<td>Datenschutz und Outsourcing – Ein neuer Ansatz</td>
<td>24</td>
</tr>
<tr>
<td>2.6</td>
<td>Outsourcing bei Trägern von Berufsgeheimnissen</td>
<td>26</td>
</tr>
<tr>
<td>2.7</td>
<td>Projekt D115 – Einheitliche Behördenruftnummer</td>
<td>27</td>
</tr>
<tr>
<td>2.8</td>
<td>Datenschutz – bloß unnötige Bürokratie?</td>
<td>29</td>
</tr>
<tr>
<td>2.9</td>
<td>Datenschutz bei Kindern – wer nimmt ihre Rechte wahr?</td>
<td>30</td>
</tr>
<tr>
<td>3</td>
<td>Wirtschaft</td>
<td>31</td>
</tr>
<tr>
<td>3.1</td>
<td>Gibt es eine Balance zwischen informationeller Selbstbestimmung und wirtschaftlichen Interessen?</td>
<td>31</td>
</tr>
<tr>
<td>3.2</td>
<td>Telekommunikations- und Teledienste</td>
<td>32</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Vorratsdatenspeicherung: Das Bundesverfassungsgericht hat das letzte Wort</td>
<td>32</td>
</tr>
</tbody>
</table>

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 21. April 2009
gemäß § 26 Absatz 1 des Bundesdatenschutzgesetzes.
3.2.2 Fall Telekom/Lehren aus dem Missbrauch von Verkehrsdaten bei der Telekom ................................................................. 33
3.2.3 Datenschutzgerechte Ausgestaltung der Auftragsdatenverarbeitung in Call-Centern ......................................................... 35
3.2.4 Nicht jeder will, doch mancher kommt auch gegen seinen Willen in das Telefonbuch .......................................................... 36
3.2.5 Bonitätsprüfung bei neuen Telefonkunden ........................................ 36
3.3 Postunternehmen ................................................................. 37
3.3.1 Anlasslose Weitergabe von Sendungsdaten in die USA ............... 37
3.3.2 Prüfungen bei Postunternehmen – Einzelfälle meiner Kontrolltätigkeit ................................................................. 38
3.4 Wirtschaft allgemein .............................................................. 38
3.4.1 Die Europäische Dienstleistungsrichtlinie und das Binnenmarktinformationssystem IMI ......................................................... 38
3.4.2 Neuer Energieausweis führt zu Ärger bei Hauseigentümern ...... 40
3.4.3 Die neue Publizitätspflicht im elektronischen Unternehmensregister und eBundesanzeiger ......................................................... 40
3.4.4 Der Mensch ist kein Score-Wert ............................................ 41
3.4.5 Informationelle Selbstbestimmung ernst nehmen – Neue Anforderungen an Werbewirtschaft und Adresshandel ............... 42
3.4.6 Datenschutz bei Rechtsanwälten weiterhin nicht gesichert ....... 42
3.4.7 Dringend notwendige Verbesserungen beim Datenschutz in der Versicherungswirtschaft lassen weiter auf sich warten ....... 43

**Freiheit und Sicherheit** ................................................................. 45

4 Innere Sicherheit ................................................................. 45
4.1 Online-Durchsuchungen durch Sicherheitsbehörden ............... 45
4.1.1 Verfassungsbeschwerde erfolgreich ........................................ 45
4.1.2 Neue Befugnisse zur Online-Durchsuchung für das BKA ........ 47
4.1.3 Online-Durchsuchungen durch Nachrichtendienste .......... 49
4.2 Veränderungen der Sicherheitsarchitektur des Bundes .......... 49
4.2.1 Bündelung der Telekommunikationsüberwachung beim Bundesverwaltungsamt ......................................................... 50
4.2.2 Anti-Terror-Datei-Gesetz ..................................................... 50
4.2.2.1 Die Protokollierung in der Anti-Terror-Datei gestaltet sich schwierig ................................................................. 51
4.2.2.2 Kontrolle der Anti-Terror-Datei beim Bundeskriminalamt ...... 51
4.2.3 Gemeinsames Analyse- und Strategiezentrum Illegale Migration (GASIM) ................................................................. 52
4.2.4 Neugestaltung der IT-Landschaft in der Abteilung Staatsschutz des Bundeskriminalamts ................................................................. 53
4.3 Bundeskriminalamt ............................................................... 53
4.3.1 BKA-Gesetzesnovelle .......................................................... 54
<table>
<thead>
<tr>
<th>Seite</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.2 Polizeiliches Informationssystem INPOL .......................... 56</td>
</tr>
<tr>
<td>4.3.2.1 Protokollierung im polizeilichen Informationssystem (INPOL) ................................................................. 56</td>
</tr>
<tr>
<td>4.3.2.2 Speicherung Strafunmündiger in INPOL .......................... 58</td>
</tr>
<tr>
<td>4.3.2.3 Noch immer keine Rechtsverordnung gemäß § 7 Absatz 6 BKAG ................................................................. 58</td>
</tr>
<tr>
<td>4.4 Bundespolizei – Noch mehr Videoüberwachung .......................... 59</td>
</tr>
<tr>
<td>4.5 Ermittlungsverfahren der Generalbundesanwaltschaft .................. 59</td>
</tr>
<tr>
<td>4.6 Bundeszentralregister beim Bundesamt für Justiz .................. 60</td>
</tr>
<tr>
<td>4.7 Nachrichtendienste .......................................................... 61</td>
</tr>
<tr>
<td>4.7.1 Bundesamt für Verfassungsschutz ....................................... 61</td>
</tr>
<tr>
<td>4.7.2 Militärischer Abschirmdienst ........................................... 61</td>
</tr>
<tr>
<td>4.7.3 Bundesnachrichtendienst ................................................ 62</td>
</tr>
<tr>
<td>4.7.3.1 Überwachung von Journalisten ...................................... 62</td>
</tr>
<tr>
<td>4.7.3.2 Auskunftsverpflichtung des BND auch bezüglich Akten ........ 63</td>
</tr>
<tr>
<td>4.8 Sicherheitsüberprüfung ..................................................... 63</td>
</tr>
<tr>
<td>4.8.1 Notwendigkeit zur Änderung des SÜG .................................. 63</td>
</tr>
<tr>
<td>4.8.2 Kontrollen ............................................................... 64</td>
</tr>
<tr>
<td>4.8.3 Sicherheitsüberprüfungen außerhalb des SÜG .......................... 64</td>
</tr>
<tr>
<td>4.8.3.1 Atomgesetz ............................................................ 65</td>
</tr>
<tr>
<td>4.8.3.2 Zuverlässigkeitsüberprüfungen ohne gesetzliche Grundlage .... 65</td>
</tr>
<tr>
<td>4.9 Rechtswesen und Innere Verwaltung ....................................... 67</td>
</tr>
<tr>
<td>4.1 Telekommunikationsüberwachung und andere heimliche Ermittlungsmaßnahmen nach der StPO .................................................. 67</td>
</tr>
<tr>
<td>4.2 Bundesmeldegesetz – Zentralregister als zentrales Problem .......... 70</td>
</tr>
<tr>
<td>4.3 Neue Ansätze in der amtlichen Statistik ................................... 72</td>
</tr>
<tr>
<td>4.4 KombiFiD ................................................................. 73</td>
</tr>
<tr>
<td>4.5 Volkszählung 2011 .......................................................... 73</td>
</tr>
<tr>
<td>4.5.1 Gesetzliche Vorgaben ................................................... 73</td>
</tr>
<tr>
<td>4.5.2 Stand der Vorbereitungen ................................................. 75</td>
</tr>
<tr>
<td>4.6 Novellierung des Bundesarchivgesetzes ................................... 75</td>
</tr>
<tr>
<td>4.7 Zentrale Einlade- und Warndatei .......................................... 76</td>
</tr>
<tr>
<td>4.8 Die Bundesbeauftragte für die Unterlagen des Staatssicherheits- dientes der ehemaligen DDR (BStU) ........................................ 77</td>
</tr>
<tr>
<td>4.9 Dopingbekämpfung .......................................................... 77</td>
</tr>
</tbody>
</table>
6 Elektronische Identität ................................................................. 78

6.1 Elektronische Gesundheitskarte ............................................. 79
6.1.1 Patientendaten im Internet – Welche Risiken verbergen sich hinter den elektronischen Gesundheitsakten und der elektronischen Fallakte? ................................................................. 80
6.1.1.1 Die elektronischen Gesundheitsakten .................................. 80
6.1.1.2 Die elektronische Fallakte .................................................. 81
6.1.2 Status „Sozialhilfeempfänger“ auf der Krankenversichertenkarte .................................................................................. 81
6.2 Die Einführung des elektronischen Entgeltnachweises (ELENA) steht bevor ................................................................. 82
6.3 Biometrie und Datenschutz ....................................................... 83
6.3.1 Elektronischer Pass der II. Generation ....................................... 84
6.3.2 Elektronischer Personalausweis ................................................. 85
6.4 Automatisierte Grenzkontrollen/Projekt GAnGes bzw. easyPass ................................................................. 86
6.5 Bundesmeldegesetz ................................................................. 87
6.6 Bürgerportale: Elektronischer Königsweg zur Verwaltung? ........ 87
6.7 RFID (Radio Frequency Identification) ......................................... 88

7 Internet ....................................................................................... 89
7.1 Geoinformationen und Datenschutz .......................................... 89
7.2 Ihr Haus im Internet? ............................................................... 90
7.3 „Super Nanny“ Datenschutz? .................................................... 91
7.4 Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums in Kraft ................................................................. 92
7.5 Die Jobbörse als Internet-Angebot der Bundesagentur für Arbeit .................................................................................. 93
7.6 Persönliche Daten im Fokus von Suchmaschinen ....................... 93
7.7 Ortung durch Handys und andere Gerätschaft ............................... 94
7.8 Verwendung von Telekommunikationsverkehrsdaten für Straßenverkehrsinformationen ................................................................. 95
7.9 Von der Schwierigkeit, Gesetze anzuwenden, am Beispiel des Telemediengesetzes ................................................................. 96
7.10 Homepage-Überwachung durch das Bundeskriminalamt .......... 96
7.11 Kontroverse: Auskunft über Inhaber von IP-Adressen ................ 97
<table>
<thead>
<tr>
<th>Seite</th>
<th>Kapitel</th>
<th>Thema</th>
</tr>
</thead>
<tbody>
<tr>
<td>99</td>
<td>8 Technologischer Datenschutz</td>
<td>8.1 Videoüberwachung</td>
</tr>
<tr>
<td>100</td>
<td></td>
<td>8.2 Verschlüsselung wichtig, aber immer noch nicht selbstverständlich</td>
</tr>
<tr>
<td>101</td>
<td></td>
<td>8.3 Effektive Datenlöschung</td>
</tr>
<tr>
<td>102</td>
<td></td>
<td>8.4 Verbesserte IT-Sicherheit – aber nicht zu Lasten des Datenschutzes!</td>
</tr>
<tr>
<td>103</td>
<td></td>
<td>8.5 Kennzeichnungspflichten – Überlegungen zur Rückverfolgung von personenbezogenen Daten</td>
</tr>
<tr>
<td>106</td>
<td>9 Finanzwesen</td>
<td>9.1 Identifikationsnummer für steuerliche Zwecke (Steuer-ID) – rechtlicher Rahmen</td>
</tr>
<tr>
<td>108</td>
<td></td>
<td>9.2 Was die Abgeltungssteuer mit der Religionszugehörigkeit zu tun hat</td>
</tr>
<tr>
<td>108</td>
<td></td>
<td>9.3 Jahressteuergesetz 2008 – Ablösung der Lohnsteuerkarte durch ein elektronisches Abruferfahren</td>
</tr>
<tr>
<td>111</td>
<td></td>
<td>9.4 Kontenabrufverfahren durch die Finanzämter und andere Behörden</td>
</tr>
<tr>
<td>111</td>
<td></td>
<td>9.5 Auskunftsanspruch in der Abgabenordnung</td>
</tr>
<tr>
<td>112</td>
<td>10 Gesundheit und Soziales</td>
<td>10.1 Das Gendiagnostikgesetz: Der Anfang ist gemacht</td>
</tr>
<tr>
<td>113</td>
<td></td>
<td>10.2 Gesetzliche Krankenversicherung</td>
</tr>
<tr>
<td>113</td>
<td></td>
<td>10.2.1 Steuerungsmaßnahmen der gesetzlichen Krankenkassen</td>
</tr>
<tr>
<td>114</td>
<td></td>
<td>10.2.2 Zusammenarbeit der gesetzlichen Krankenkassen mit privaten Dritten</td>
</tr>
<tr>
<td>116</td>
<td></td>
<td>10.2.3 Keine Extra-Daten für den Risikostrukturausgleich</td>
</tr>
<tr>
<td>116</td>
<td></td>
<td>10.2.4 Schwere Verstöße von Krankenkassen bei der Vermittlung privater Zusatzversicherungen</td>
</tr>
<tr>
<td>117</td>
<td></td>
<td>10.3 Gesetzliche Unfallversicherung</td>
</tr>
<tr>
<td>117</td>
<td></td>
<td>10.3.1 Gutachterregelung</td>
</tr>
<tr>
<td>118</td>
<td></td>
<td>10.3.2 Einschränkung des Auskunftsverlangens bei Krankenkassen nach § 188 Satz 2 SGB VII</td>
</tr>
<tr>
<td>118</td>
<td></td>
<td>10.4 Gesetzliche Rentenversicherung</td>
</tr>
<tr>
<td>119</td>
<td></td>
<td>10.4.1 Der ärztliche Entlassungsbericht in der medizinischen Rehabilitation – wer darf ihn bekommen?</td>
</tr>
<tr>
<td>119</td>
<td></td>
<td>10.5 Arbeitsverwaltung</td>
</tr>
<tr>
<td>119</td>
<td></td>
<td>10.5.1 Die Jobbörse der Bundesagentur für Arbeit in der Kritik</td>
</tr>
<tr>
<td>Seite</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.5.2 Erhebung des Migrationshintergrunds von Arbeitsuchenden geplant</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>10.5.3 Noch kein neuer Sachstand bei der datenschutzrechtlichen Aufsicht für die Arbeitsgemeinschaften (ARGE)</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>10.5.4 Einzelfälle</td>
<td>121</td>
<td></td>
</tr>
<tr>
<td><strong>11 Mitarbeiterdatenschutz</strong></td>
<td>122</td>
<td></td>
</tr>
<tr>
<td>11.1 Dringender Handlungsbedarf beim Arbeitnehmerdatenschutz</td>
<td>122</td>
<td></td>
</tr>
<tr>
<td>11.2 Angehörige erhalten ein eigenes Antragsrecht bei der Beihilfe</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>11.3 Bewerbungsunterlagen sind nach zwei Monaten zurückzugeben oder zu vernichten</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>11.4 Nicht alle Aufgaben eignen sich für Telearbeit</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td><strong>12 Verkehr</strong></td>
<td>124</td>
<td></td>
</tr>
<tr>
<td>12.1 Verwendung der Mautdaten zur Strafverfolgung?</td>
<td>124</td>
<td></td>
</tr>
<tr>
<td>12.2 Neues Maritimes Sicherheitszentrum soll Zusammenarbeit verbessern</td>
<td>124</td>
<td></td>
</tr>
<tr>
<td>12.3 Online-Anbindung der örtlichen Fahrerlaubnisbehörden an das Zentrale Fahrerlaubnisregister des Kraftfahrt-Bundesamtes</td>
<td>124</td>
<td></td>
</tr>
<tr>
<td><strong>13 Europa und Internationales</strong></td>
<td>125</td>
<td></td>
</tr>
<tr>
<td>13.1 Europäische Rechtsentwicklung</td>
<td>125</td>
<td></td>
</tr>
<tr>
<td>13.2 Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie</td>
<td>125</td>
<td></td>
</tr>
<tr>
<td>13.2.1 Gemeinsame Aktivitäten: Europaweite Datenschutzprüfung im Krankenversicherungssektor</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>13.2.2 Safe Harbor</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>13.2.3 Binding Corporate Rules</td>
<td>126</td>
<td></td>
</tr>
<tr>
<td>13.2.4 Stellungnahme zu personenbezogenen Daten</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td>13.3 Europaweite Zusammenarbeit von Polizei- und Sicherheitsbehörden und von Datenschutzkontrollbehörden</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>13.3.1 Rahmenbeschluss über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen</td>
<td>129</td>
<td></td>
</tr>
<tr>
<td>13.3.2 Vertrag von Prüm und dessen Überführung in europäisches Recht</td>
<td>129</td>
<td></td>
</tr>
<tr>
<td>13.3.3 EUROPOL</td>
<td>130</td>
<td></td>
</tr>
<tr>
<td>13.3.4 Schengen</td>
<td>131</td>
<td></td>
</tr>
<tr>
<td>13.3.5 Zugriff der Sicherheitsbehörden auf das Visa-Informationsystem</td>
<td>133</td>
<td></td>
</tr>
<tr>
<td>Seite</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>133</td>
<td></td>
<td></td>
</tr>
<tr>
<td>135</td>
<td></td>
<td></td>
</tr>
<tr>
<td>135</td>
<td></td>
<td></td>
</tr>
<tr>
<td>136</td>
<td></td>
<td></td>
</tr>
<tr>
<td>138</td>
<td></td>
<td></td>
</tr>
<tr>
<td>138</td>
<td></td>
<td></td>
</tr>
<tr>
<td>139</td>
<td></td>
<td></td>
</tr>
<tr>
<td>139</td>
<td></td>
<td></td>
</tr>
<tr>
<td>140</td>
<td></td>
<td></td>
</tr>
<tr>
<td>141</td>
<td></td>
<td></td>
</tr>
<tr>
<td>141</td>
<td></td>
<td></td>
</tr>
<tr>
<td>142</td>
<td></td>
<td></td>
</tr>
<tr>
<td>143</td>
<td></td>
<td></td>
</tr>
<tr>
<td>143</td>
<td></td>
<td></td>
</tr>
<tr>
<td>144</td>
<td></td>
<td></td>
</tr>
<tr>
<td>144</td>
<td></td>
<td></td>
</tr>
<tr>
<td>144</td>
<td></td>
<td></td>
</tr>
<tr>
<td>144</td>
<td></td>
<td></td>
</tr>
<tr>
<td>144</td>
<td></td>
<td></td>
</tr>
<tr>
<td>145</td>
<td></td>
<td></td>
</tr>
<tr>
<td>145</td>
<td></td>
<td></td>
</tr>
<tr>
<td>145</td>
<td></td>
<td></td>
</tr>
<tr>
<td>146</td>
<td></td>
<td></td>
</tr>
<tr>
<td>147</td>
<td></td>
<td></td>
</tr>
<tr>
<td>147</td>
<td></td>
<td></td>
</tr>
<tr>
<td>148</td>
<td></td>
<td></td>
</tr>
<tr>
<td>148</td>
<td></td>
<td></td>
</tr>
<tr>
<td>149</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13.3.6 Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten

13.3.7 Kontrolle der EU-Außengrenzen

13.3.8 Tätigkeit der Datenschutzkontrollgremien

13.4 Deutsch-amerikanisches Regierungsabkommen zur Bekämpfung schwerwiegender Kriminalität

13.5 Fluggastdaten

13.5.1 Übermittlung von Flugpassagierdaten (PNR)

13.5.2 PNR USA

13.5.3 Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdaten (PNR-Daten) zu Strafverfolgungszwecken

13.5.4 Umsetzung der Richtlinie 2004/82/EG zur Übermittlung von Fluggastdaten

13.6 Listen der Vereinten Nationen und der Europäischen Union über Terror verdächtige

13.7 Datenübermittlungen des Bundeskriminalamtes an Behörden der Russischen Föderation

13.8 Die Europäische Frühjahrskonferenz

13.9 Die Internationale Datenschutzkonferenz

14 Andere Bereiche

14.1 Übermittlung von Gesundheitsdaten an Versicherungen

14.2 Unzureichender Datenschutz in einer Auslandsvertretung

15 Aus meiner Dienststelle

15.1 Konferenz der Datenschutzbeauftragten des Bundes und der Länder

15.2 Europäischer Datenschutztag

15.3 25 Jahre Volkszählungsurteil

15.4 Bad Godesberger Symposien zum Datenschutz in der Telekommunikation und im Internet

15.5 Zusammenarbeit mit den behördlichen Datenschutzbeauftragten

15.6 Zusammenarbeit mit den Aufsichtsbehörden

15.7 Die Internationale Datenschutzkonferenz 2008

15.8 Öffentlichkeitsarbeit

15.9 Mehr Präsenz in der Bundeshauptstadt
15.10  BfDI als Ausbildungsbehörde .......................... 149
15.11  Zusätzliches Personal dringend erforderlich .......... 149

16  Wichtiges aus zurückliegenden Tätigkeitsberichten ...... 151
1.  Gesetz zur Umsetzung aufenthalts- und asylrechtlicher Richtlinien der Europäischen Union .................. 151
2.  Europäisches Visa-Informationssystem (VIS) ............. 151
3.  Datenerhebung zu Forschungszwecken ohne Rechtsgrundlage . 151
4.  Suchdienstdatenschutzgesetz (SDDSG) ..................... 151
5.  Entwurf des Zweiten Gesetzes zur Änderung des Vierten Buches Sozialgesetzbuch und anderer Gesetze, wie z. B. des Schwarzarbeitsbekämpfungsgesetzes (SchwarzArbG) .... 151
6.  Erhebungs- und Leistungssystem A2LL bei der BA .......... 152
7.  Unzulässige Datensammlung der BA über die Nutzer der BA-Internet-Plattform ........................................ 152
8.  Zentrales Vorsorgeregister bei der Bundesnotarkammer .... 152
9.  Online-Angebot „Öffentliche Petition“ ...................... 152
10.  Projekt HERKULES .................................. 152
12.  Vertragsloser Zustellungsverkehr ............................ 152
13.  Entlassungsberichte aus Rehabilitationseinrichtungen .... 153
14.  EPOS 2.0 ........................................ 153
15.  Dienstrechtsneuordnungsgesetz .............................. 153
16.  Express- und Paketzustelldienst UPS ...................... 153
17.  Übermittlung flugmedizinischer Daten an das Luftfahrt-Bundesamt (LBA) ................................................ 153
18.  Telematikverfahren für Kraftfahrzeuge ....................... 153
19.  Wissenschaftsserver ..................................... 154
20.  SWIFT ........................................ 154
21.  Verarbeitung erkennungsdienstlicher Unterlagen im Bundeskriminalamt ........................................ 154
22.  Geldwäsche ........................................ 154
23.  Zollfahndungsdienstegesetz ................................. 154
24.  Akustische Wohnraumüberwachung ....................... 155
25.  Unterdrückte Rufnummer ............................... 155
Im Tätigkeitsbericht sind nur die Entschließungen abgedruckt, auf die in den Beiträgen unmittelbar Bezug genommen wird. Alle Entschließungen der Datenschutzkonferenzen und weitere Informationen finden Sie auf der Internet-Seite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.bfdi.bund.de.

Anlage 1
Hinweise für die Ausschüsse des Deutschen Bundestages .................. 157

Anlage 2
Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche ......................................................... 158

Anlage 3
Übersicht über Beanstandungen nach § 25 BDSG ........................... 160

Anlage 4

Anlage 5

Anlage 6

Anlage 7
30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre vom 15. bis 17. Oktober 2008 Entschließung zum Datenschutz in Sozialen Netzwerkdiensten ........ 170

Anlage 8
30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre vom 15. bis 17. Oktober 2008 Entschließung zum Schutz der Privatsphäre von Kindern im Internet ...... 173

Anlage 9
Erklärung der Europäischen Datenschutzkonferenz von Zypern, angenommen am 11. Mai 2007 ................................................. 175

Anlage 10
Erklärung der Europäischen Datenschutzkonferenz vom 16. bis 18. April 2008 in Rom ............................................................. 177

Organigramm der Dienststelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ................................. 178

Sachregister ................................................................................. 179

Abkürzungsverzeichnis/Begriffe .................................................. 185
Kasten zu Nr. 2.1
75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008:

Kasten zu Nr. 2.2
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008:
Entschlossenes Handeln ist das Gebot der Stunde .................. 20

Kasten a zu Nr. 2.3
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008:
Adress- und Datenhandel nur mit Einwilligung der Betroffenen ........ 22

Kasten b zu Nr. 2.3
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008:
Mehr Transparenz durch Informationspflichten bei Datenschutzpannen ... 22

Kasten c zu Nr. 2.3
Gesetzesinitiativen der Bundesregierung zu Auskunfteien und Scoring:
Nachbesserung bei Auskunfteiregelungen gefordert .................... 23

Kasten zu Nr. 2.5
Kernaussagen des Arbeitspapiers „Datenschutzrechtliche Grundlagen bei Auftragsdatenverarbeitung/Outsourcing“ .......................... 25

Kasten zu Nr. 2.6
§ 203 Strafgesetzbuch .................................................................. 27

Kasten zu Nr. 2.7
Netzeinrichtung ............................................................................. 29

Kasten zu Nr. 2.9
Beispiele für Konflikt situationen .................................................. 31

Kasten zu Nr. 3.2.1
Vorratsdatenspeicherung ............................................................... 32

Kasten zu Nr. 3.2.3
Datenschutzgerechte Ausgestaltung der Auftragsdatenverarbeitung in Call-Centern .......................................................... 35

Kasten zu Nr. 3.4.1
Binnenmarktinformationssystem IMI .............................................. 39

Kasten zu Nr. 3.4.6
Aus der Stellungnahme der Bundesregierung zum 21. TB zu Nr. 9.7 ...... 42

Kasten zu Nr. 4.1
Online-Durchsuchung .................................................................. 45

Kasten zu Nr. 4.1.1
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008:
Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten ......................................................... 46

Kasten zu Nr. 4.1.2
§ 20k BKA-Gesetz ........................................................................... 48
Kasten a zu Nr. 4.3.1
Ergebnis der Förderalismusreform .............................................. 54

Kasten b zu Nr. 4.3.1
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes
und der Länder am 3./4. April 2008:
Mehr Augenmaß bei der Novellierung des BKA-Gesetzes ............... 55

Kasten a zu Nr. 4.3.2.1
Verfahren zur Protokollierung von Datenabrufen im polizeilichen
Informationssystem INPOL .......................................................... 56

Kasten b zu Nr. 4.3.2.1
Gesetzliche Regelungen zur Protokollierung von Datenabrufen aus
Informationssystemen ............................................................... 57

Kasten zu Nr. 4.3.2.2
§ 8 Absatz 5 BKA-Gesetz ............................................................. 58

Kasten zu Nr. 4.7.2
§ 6 Absatz 2 MADG ................................................................. 61

Kasten a zu Nr. 4.8.3.2
Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes
und der Länder vom 25./26. Oktober 2007:
Zuverlässigkeitsüberprüfungen bei Großveranstaltungen ............... 66

Kasten b zu Nr. 4.8.3.2
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes
und der Länder am 3./4. April 2008:
Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung
von Arbeitnehmerinnen und Arbeitnehmern .............................. 66

Kasten a zu Nr. 5.1
Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes
und der Länder vom 8./9. März 2007:
Vorratsdatenspeicherung, Zwangidentifikation im Internet, Telekommuni-
kationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen .... 68

Kasten b zu Nr. 5.1
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes
und der Länder am 6./7. November 2008:
Abfrage von Telekommunikationsverkehrsdaten einschränken:
Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen
Konsequenzen ziehen .............................................................. 69

Kasten zu Nr. 5.2
Gemeinsames Eckpunktepapier der Datenschutzbeauftragten des Bundes
Datenschutzrechtliche Forderungen für ein Bundesmeldegesetz ........ 71

Kasten a zu Nr. 5.5.1
Zensusarbeiten nach dem geplanten ZensG 2011 .......................... 74

Kasten b zu Nr. 5.5.1
Anforderungen der EU-Zensusverordnung .................................. 74

Kasten zu Nr. 5.9
Zur Datenbank ADAMS ............................................................ 78
<table>
<thead>
<tr>
<th>Kasten zu Nr. 6</th>
<th>Identitätsmanagement (IDM)</th>
<th>78</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kasten b zu Nr. 6</td>
<td>Mindestforderungen beim Identitätsmanagement (IDM)</td>
<td>79</td>
</tr>
<tr>
<td>Kasten zu Nr. 6.1</td>
<td>Zwiebelschalenmodell des Basis-Rollouts</td>
<td>79</td>
</tr>
<tr>
<td>Kasten zu Nr. 6.2</td>
<td>Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008: Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren</td>
<td>83</td>
</tr>
<tr>
<td>Kasten zu Nr. 6.6</td>
<td>Bürgerportalgesetz</td>
<td>88</td>
</tr>
<tr>
<td>Kasten zu Nr. 7.1</td>
<td>Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008: Datenschutzgerechter Zugang zu Geoinformationen</td>
<td>90</td>
</tr>
<tr>
<td>Kasten zu Nr. 7.2</td>
<td>Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich am 13./14. November 2008 Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet</td>
<td>91</td>
</tr>
<tr>
<td>Kasten zu Nr. 7.3</td>
<td>Die Zehn Gebote für Betreiber sozialer Netzwerke</td>
<td>91</td>
</tr>
<tr>
<td>Kasten zu Nr. 7.6</td>
<td>Anforderungen an Suchmaschinen</td>
<td>94</td>
</tr>
<tr>
<td>Kasten zu Nr. 7.8</td>
<td>In der Telekommunikation unterscheidet man verschiedene Arten von Daten</td>
<td>95</td>
</tr>
<tr>
<td>Kasten a zu Nr. 8</td>
<td>Stichwort Sicherheitsziele</td>
<td>99</td>
</tr>
<tr>
<td>Kasten b zu Nr. 8</td>
<td>Vorschlag für eine Charta des digitalen Datenschutzes und der Informationsfreiheit</td>
<td>100</td>
</tr>
<tr>
<td>Kasten zu Nr. 8.1</td>
<td>Video-Infozeichen nach DIN 33450</td>
<td>101</td>
</tr>
<tr>
<td>Kasten zu Nr. 8.3</td>
<td>Keine persönlichen Daten auf ausrangierten PC vergessen! Tipps zur Vermeidung einer bösen Überraschung</td>
<td>103</td>
</tr>
<tr>
<td>Kasten zu Nr. 8.4</td>
<td>Gesetzentwurf zur Stärkung der Sicherheit in der Informationstechnik des Bundes</td>
<td>104</td>
</tr>
<tr>
<td>Kasten zu Nr. 8.5</td>
<td>Technische Verfahren zur Kennzeichnung von Daten</td>
<td>105</td>
</tr>
<tr>
<td>Kasten zu Nr. 9.1</td>
<td>Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008: Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen</td>
<td>107</td>
</tr>
</tbody>
</table>
Kasten a zu Nr. 9.3
Zentrale Steuerdatei droht zum Datenmölchen zu werden .......................... 109

Kasten b zu Nr. 9.3
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008:
Elektronische Steuererklärung sicher und datenschutzgerecht gestalten ... 110

Kasten zu Nr. 9.5

Kasten zu Nr. 10.2.1
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008:
Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten ................................................................. 114

Kasten a zu Nr. 10.2.2
§ 80 Absatz 5 SGB X ............................................................. 115

Kasten b zu Nr. 10.2.2
§ 197b SGB V ................................................................. 115

Kasten a zu Nr. 10.3.1
Kernsätze des Urteils des BSG vom 5. Februar 2008 – B 2 U 8/07 R – zu datenschutzrechtlich relevanten Fragen ......................................................... 117

Kasten b zu Nr. 10.3.1
Vorschlag für eine geänderte datenschutzfördernde Fassung des § 200 Absatz 2 SGB II ................................................................. 118

Kasten zu Nr. 10.4
Der Reha-Entlassungsbericht ............................................................. 119

Kasten zu Nr. 11.1
Forderungen an ein Arbeitnehmerdatenschutzgesetz ............................. 122

Kasten zu Nr. 13.2
Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie .... 126

Kasten zu Nr. 13.2.4
Der Begriff der „personenbezogenen Daten“ in der Richtlinie 95/46/EG ... 127

Kasten zu Nr. 13.3
Rechtsakte .................................................................................. 128

Kasten zu Nr. 13.3.2
Der Vertrag von Prüm .................................................................... 130

Kasten zu Nr. 13.3.4
Das Schengener Informationssystem (SIS) ........................................ 132

Kasten zu Nr. 13.3.6
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008:
Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten .................................................. 134
Kasten zu Nr. 13.4
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008:
Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden .......................... 137

Kasten a zu Nr. 13.5.1
Unterrichtung der Fluggäste ........................................ 138

Kasten b zu Nr. 13.5.1
Forderung nach globalen Standards ................................. 138

Kasten zu Nr. 13.5.3
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008:
Keine Vorratsspeicherung von Flugpassagierdaten .................. 140

Kasten zu Nr. 15.3
Aus dem Festvortrag von Herrn Professor Dr. Papier anlässlich der Veranstaltung zum 25. Jahrestag der Verkündung des Volkszählungsurteils ................................. 146

Kasten zu Nr. 15.6

Kasten zu Nr. 15.8
Nutzerzahlen der Internet-Seite www.bfdi.bund.de .................. 149

Kasten zu Nr. 15.11
Statistische Auswertung .................................................. 150
Einführung


Ohne deutliche Personalverstärkung wird die Arbeit in der Zukunft nicht mit gleicher Intensität und Qualität fortgesetzt werden können.

Peter Schaar
Zur Lage des Datenschutzes in Deutschland


Die Bilanz der letzten beiden Jahre fällt in dieser Hinsicht eher gemischt aus:


Auch sonst war die datenschutzrechtliche Diskussion im öffentlichen Bereich vielfach vom Spannungsverhältnis zwischen den Belangen der inneren Sicherheit und dem Grundrecht auf informationelle Selbstbestimmung geprägt: Die Vorratsdatenspeicherung (vgl. Nr. 3.2.1), die BKA-Gesetzesnovelle (vgl. Nr. 4.3.1) oder auch die europaweite Zusammenarbeit von Polizei- und Sicherheitsbehörden (vgl. Nr. 13.3) können hier als Beispiele genannt werden.

Daneben gibt es aber noch weitere wichtige Themen: Hierzu gehören die Auseinandersetzung um das Bundesmeldegesetz und ein zentrales Melderegister (vgl. Nr. 5.2; 6.5) ebenso wie die Vorbereitung der Volkszählung 2011 (vgl. Nr. 5.4) oder die Umsetzung der Europäischen Dienstleistungsrichtlinie und das Binnenmarktinformationssystem IMI (vgl. Nr. 3.4.1).


Im nicht-öffentlichen Bereich, also beim Datenschutz in der Wirtschaft, war die Debatte von einer Reihe von Skandalen geprägt, die in dieser Häufigkeit bislang nicht für möglich gehalten wurden und nachdrücklich die enormen Defizite ins Bewusstsein rückten, die hier beim Umgang mit persönlichen Daten offensichtlich bestehen. Viele der Probleme und Fehlentwicklungen, die diese Skandale erst möglich gemacht haben, waren den Fachleuten durchaus bekannt, aber ihre jahrelangen Hinweise und Warnungen verhallten weithin ungehört. Erst der eklatante Missbrauch, der Skandal konnte das Interesse der Medien und der Öffentlichkeit wecken.

Ich selbst war unmittelbar durch die Ereignisse bei der Deutschen Telekom AG betroffen, da ich hier die datenschutzrechtliche Aufsicht führte (vgl. Nr. 3.2.2). Obwohl die staatsanwaltschaftlichen Ermittlungen und auch meine eigenen Untersuchungen noch nicht abgeschlossen sind, hat sich bereits erwiesen, dass die datenschutzrechtliche Organisation im Konzern nicht im vollen Umfang den gesetzlichen Anforderungen entsprochen hat. Die Skandale bei Lidl und anderen Handelsunternehmen und
die Massenüberprüfungen bei den Beschäftigten der Deutschen Bahn haben wohl auch dem letzten Zweifler vor Augen geführt, wie es um den Arbeitnehmerdatenschutz in Deutschland steht. Der Deutsche Bundestag hat seit vielen Jahren immer wieder einstimmig die Vorlage eines Arbeitnehmerdatenschutzgesetzes gefordert (vgl. Nr. 11.1), bislang ohne Erfolg. Als Reaktion auf den offens zu Tage getretenen Missbrauch soll jetzt gehandelt wer-
den. Ich hoffe, dass es nicht wieder bei Ankündigungen bleibt und gesetzgeberische Taten folgen.

Die aufgedeckten Missstände beim Handel mit personenbezogenen Daten und die illegale Weitergabe von Konto-
verbindungen und anderen geschützten persönlichen Da-
ten haben zu einem Spitzengespräch der betroffenen
Bundesminister und der Datenschutzaufsichtsbehörden
geführt (vgl. Nr. 2.2), bei dem wichtige Änderungen für
den Datenhandel verabredet wurden. Den betroffenen
Bürgerinnen und Bürgern soll ein Stück weit die Ent-
scheidung über den Umgang mit ihren persönlichen Da-
ten zurückgegeben werden. Die Bundesregierung hat
hierzu im Dezember 2008 einen Gesetzentwurf vorgelegt,
der derzeit in den parlamentarischen Gremien behandelt
wird (vgl. Nr. 2.3 und 3.4.5). Ein weiterer Gesetzentwurf
soll den Datenschutz bei Score-Verfahren und im Aus-
kunfteiwesen verbessern (Nr. 2.3 und 3.4.4).

So wichtig diese angestrebten Verbesserungen im Detail sind, dürfen sie doch nicht darüber hinwegtäuschen, dass die Modernisierung des Datenschutzrechts in seiner Struktur und in seinen grundlegenden Regelungsmecha-
nismen heute dringender ist denn je.

Beim Eintritt in das Zeitalter allgegenwärtiger Datenver-
arbeitung („ubiquitous computing“) erweisen sich die
hergebrachten Begriffe des Datenschutzrechts (verant-
wortliche Stelle, Auftragnehmer, personenbezogene Da-
ten) genauso als diskussionsbedürftig wie die dem Daten-
enschutzrecht zu Grunde liegenden Prinzipien, etwa die
Konzepte der Erforderlichkeit oder der Zweckbindung
und seine Aufsplitterung in eine Vielzahl von Rechtsvor-
schriften.

Bereits vor gut zehn Jahren wurde eine intensive Diskus-
ion über die Modernisierung des Datenschutzrechts geführt, deren immer noch lesenswerte Ergebnisse (insbesonde-
er das „Professorugutachten“ von Garstka, Roßna-
gel und Pfitzmann) Ende 2001, unmittelbar nach ihrer Er-
stellung, allerdings in einer Ministeriumsschublade
landeten und inzwischen einigen Staub angesetzt haben
dürften. In der damaligen politischen Stimmungslage, die
gegrapt war durch die Terroranschläge am 11. Septem-
tober 2001, erschien der Datenschutz Vielen bestenfalls
nachrangig, vielfach sogar eher hinderlich. Zum Versan-
temperatur, „wer was über ihn weiß“. Diese Maxime ist al-
erdings unter den Bedingungen des Internets und der
allgegenwärtigen Datenverarbeitung, wo Daten quasi als
Nebenprodukte der Kommunikation oder der Erbringung
irgendwelcher Dienstleistungen entstehen, heute unrealis-
tischer denn je. Die zunehmende Komplexität technologi-
scher Systeme erschwert die Herstellung von Transparenz
im Sinne einer umfassenden Kenntnis des Betroffenen
hinsichtlich der zu seiner Person verarbeiteten Daten.
Umso wichtiger ist eine Komplexitätsreduktion, bei der
die wesentlichen Informationen vermittelt und dem Ein-
zellen eine faktische Möglichkeit zur Entscheidung über
echte Alternativen gegeben wird. Immer umfangreichere
Datenschutzinformationen und Einwilligungsklauseln be-
wirken eher das Gegenteil: sie werden meistens nicht ein-
mal zur Kenntnis genommen, sondern bloß abgehakt in
die Hoffnung, es werde schon nichts passieren. So wün-
schenswert eine möglichst hohe Granularität der von den
Betroffenen einzustellenden Systemparameter sein mag,
sind doch die meisten Nutzer damit ihre Hoffnungen
überfordert. Von entscheidender Bedeutung wird es deshalb sein, die Grundeinstellung technologischer Systeme
datenschutzfreundlich zu gestalten, das heißt, sie auf Daten-
vermeidung und Datensparsamkeit auszulegen (vgl.
Nr. 8 ff.).

Schließlich darf nicht vergessen werden, dass die wesent-
lchen Wertentscheidungen unserer Gesellschaft in der
Verfassung niedergelegt sind. In der demokratischen In-
formationsgesellschaft gehört das Schutz des Rechts
auf informationelle Selbstbestimmung auch explizit Ver-
fassungsrecht. Es überzeugt einfach nicht, dass diejeni-
gen, die Artikel 13 (Unverletzlichkeit der Wohnung) und Artikel 16 GG (Asylrecht) im Stile einer Verwaltungsvorschrift ergänzt haben, um diese Grundrechte einzuschränken, nun gegen die Aufnahme des Datenschutzes in die Verfassung damit argumentieren, man dürfe dieselbe nicht unnötig aufblühen.


2 Datenschutzrechtlicher Rahmen

2.1 Weiterentwicklung des Datenschutzes

Die grundlegende Modernisierung des Datenschutzes wird weiter verschoben. Initiativen gibt es nur zu einzelnen Bereichen.


Gleichwohl war die seit meinem letzten Tätigkeitsbericht verstrichene Zeit nicht nur von Stillstand gekennzeichnet.


Deutscher Bundestag – 16. Wahlperiode – 19 –

Drucksache 16/12600

Kasten zu Nr. 2.1

75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Berlin Erklärung:
Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts


Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es die Wirtschaft etwa darum, durch Scoring-Verfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten als verdächtig angesehen, was die Verwaltung in die Geschäftsführung des Datenschutzgesetzes. Angesichts der stetig fortschreitenden technischen Entwicklung ist die Erfüllung dieser verfassungsgerichtlichen Verpflichtung ein dynamischer, d. h. fortwährender Prozess. Ich hoffe, dass die Konsequenzen aus dieser weit reichenden Entscheidung von den politisch Verantwortlichen erkannt und zügig umgesetzt werden.

Die Bundesregierung hat punktuell datenschutzrechtliche Probleme aufgegriffen. So hat sie im Sommer 2008 den Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Bundestagsdrucksache 16/10529) in das Gesetzgebungsverfahren eingebracht, durch das Scoring-Verfahren für die betroffenen Bürgerinnen und Bürger transparenter und die Tätigkeit von Auskunftseiten besser geregelt werden sollen (vgl. Nr. 2.3 und Nr. 3.4.4).

Als Reaktion auf die 2008 bekannt gewordenen Missstände beim Handel mit personenbezogenen Daten hat die Bundesregierung in einem weiteren, vom Kabinett am 10. Dezember 2008 beschlossenen Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften (Bundesratsdrucksache 4/09) eine Reihe von Änderungen im BDSG und die Einführung eines bundesweiten Datenschutzaudits vorgesehen (vgl. Nr. 2.3, 2.4, 3.4.5).

Damit ist zwar insgesamt Bewegung in die datenschutzrechtlichen Regelungen gekommen, was ich durchaus begrüße. Diese notwendigen Änderungen im Detail können aber eine grundlegende Überarbeitung des Datenschutzes einschließlich seiner Kontroll- und Sanktionsmechanismen nicht ersetzen. Die Forderung nach einer grundlegenden Revision verliert deswegen nicht an Bedeutung, sondern wird noch dringlicher.


2.2 Der „Datenschutzgipfel“ und seine Folgen


Entschlossenes Handeln ist das Gebot der Stunde


Es ist dringend erforderlich, dass die Politik und die Gesellschaft ihre Verantwortung für den Schutz der privaten Daten der Bürgerinnen und Bürger übernehmen und eine neue Datenschutzkultur entwickeln. Dazu ist es erforderlich, dass die Datenschutzbeauftragten der Bundesländer und des Bundes eine stärkere Rolle in der Überwachung und Kontrolle der Datensammlungen und -übertragungen spielen, um sicherzustellen, dass die Datenschutzbestimmungen eingehalten werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachzukommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

- Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren
- Stärkung der datenschutzrechtlichen Auskunftsrechte
- Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung
- Gewinnabspaltung aus unbefugtem Datenhandel
- Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird
- Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle
- Spezialisierung der Strafverfolgungsbehörden
- Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.
brauch bis dahin nur den Datenschutzaufsichtsbehörden bekannt, deren wiederholte Hinweise und Warnungen un­gehört verhallten, rückte das Thema plötzlich in die Schlagzeilen und sensibilisierte viele Menschen dafür, wie gefährdet auch ihre Privatsphäre und ihre personen­bezogenen Daten sind.


- Daten sollen für Werbezwecke nur noch nach Einwilligung des Betroffenen weitergegeben werden
- Einführung eines gesetzlichen Koppelungsverbots für marktbeherrschende Unternehmen
- Erweiterung der Bußgeldtatbestände für Datenschutz­verstöße
- Schaffung einer Möglichkeit, unrechtmäßig erworbene Gewinne aus illegaler Datenverwendung abzuschöpfen zu können.

Zusätzlich ergingen Prüfaufträge zu folgenden Punkten:

- Stärkung der betrieblichen Datenschutzbeauftragten,
- Einführung einer Kennzeichnungspflicht für die Herkunft personenbezogener Daten,
- Einführung einer Informationspflicht bei Datenschutz­pannen.

Weiter kündigte der Bundesminister des Innern die Vorlage eines Datenschutzauditgesetzes an.


Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beteiligte sich an der Diskussion und verabschiedete am 16. September 2008 eine Ent­schließung, die die Konsequenzen auflistet, die aus den Skandalen zu ziehen sind (vgl. Kasten zu Nr. 2.2).

### 2.3 Datenschutz in der Privatwirtschaft – zwei Gesetzesnovellen sollen die Rechte der Betroffenen stärken

Im Berichtszeitraum rückte der Datenschutz in der Pri­vatwirtschaft in den Fokus. Gleich zwei Gesetzentwürfe sollen hier für mehr Transparenz und besseren Schutz personenbezogener Daten sorgen.

Entsprechend den Ergebnissen des Spitzentreffens hat das Bundesministerium des Innern im September 2008 einen ersten Diskussionsentwurf zur Änderung des BDSG vor­gelegt. Während Artikel 1 des Entwurfs das angekündigte Datenschutzauditgesetz enthält (vgl. hierzu Nr. 2.4), sieht Artikel 2 als wichtigste Regelungen die grundsätzliche Abschaffung des sog. „Listenprivilegs“ in § 28 Absatz 3 Nummer 3 und ein Verbot für marktbeherrschende Unternehmen vor. Vertragsabschlüsse an die Einwilligung des Vertragspartners in die Weitergabe seiner personenbezogenen Daten zu Werbezwecken zu koppeln (Koppelungs­verbot). Außerdem sollten die Bußgeldtatbestände für Datenschutzverstöße erweitert und der Bußgeldrahmen erhöht werden, verbunden mit der Möglichkeit, zur Abschöpfung unrechtmäßig erworbener Gewinne aus illegaler Datenverarbeitung im Einzelfall den Bußgeldrahmen auch überschreiten zu können. Von den erteilten Prüfaufträgen wurde die Stärkung der betrieblichen Datenschutz­beauftragten durch die Einführung eines besonderen Kündigungsschutzes und die Einführung einer Informationspflicht bei Datenschutz­pannen berücksichtigt, wenn auch unter einschränkenden Bedingungen (vgl. zur inhalt­lichen Bewertung auch Nr. 3.4.5). Einzig die Pflicht, die Herkunft personenbezogener Daten zu kennzeichnen, fand keinen Eingang in den Entwurf, möglicherweise auch deshalb, weil Unsicherheit über die technische Realisierbarkeit dieses Vorschlags bestand (vgl. auch Nr. 8.5).

Dieses Gesetzgebungsvorhaben fand zwar viel Zuspruch in der Öffentlichkeit, stieß aber auch auf heftige Kritik der betroffenen wirtschaftlichen Kreise, die in teils drastischen Stellungnahmen auf ihrer Ansicht nach zu erwartende Auswirkungen auf Unternehmen und Arbeitsplätze hinwiesen. Die Proteste waren so heftig, dass ein Abrüchen von diesem Vorhaben nicht mehr ausgeschlossen werden konnte.


Trotz des heftigen Lobbydrucks beschloss die Bundes­regierung am 10. Dezember den Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung des Datenschutzrechtlicher Vorschriften (Bundesratsdrucksache 4/09), der trotz zahlreicher Änderungen und Ergän­zungen in Einzelpunkten im Kern dem ursprünglichen

---

Drucksache 16/12600

Deutscher Bundestag – 16. Wahlperiode – 21 –
Gesetzentwurf des BMI entspricht. Ich hoffe sehr, dass jetzt auch Bundesrat und Bundestag dem Vorhaben zustimmen werden und dieses ohne weitere Abstriche noch in dieser Legislaturperiode verabschiedet werden kann. Es wäre der Öffentlichkeit nicht zu vermitteln, wenn dieses wichtige Gesetzesvorhaben, das die Konsequenz aus millionenfächernem Datenmissbrauch zieht und den Bürgerinnen und Bürgern die Verfügungsmacht über ihre personenbezogenen Daten ein Stück weit zurückgeben will, doch noch am Widerstand derer scheitern sollte, die erhebliche Gewinne dadurch erzielen, dass sie ohne Zustimmung der Betroffenen mit deren Daten Handel treiben.

**Kasten a zu Nr. 2.3**

**Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008**

**Adress- und Datenhandel nur mit Einwilligung der Betroffenen**


Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.


Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.


Bereits im Sommer 2007 hatte die Bundesregierung ein Gesetz zur Änderung des Bundesdatenschutzgesetzes (Bundestagsdrucksache 16/10529) auf den Weg gebracht, das zu mehr Transparenz bei Scoring-Verfahren und klaren Regelungen für Auskunftsfreiheit sorgen soll. Nachdem ich in früheren Tätigkeitsberichten immer wieder auf datenschutzrechtliche Probleme bei Auskunftsfreiheit und Score-Verfahren hingewiesen hatte, forderte der Deutsche


**Gesetzesinitiativen der Bundesregierung zu Auskunftseiten und Scoring: Nachbesserung bei Auskunftseitenregelungen gefordert**


Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunftseiten zu überarbeiten und neue Regelungen zum Scoring zu schaffen.


2.4 Neuer Anlauf für ein bundesweites Datenschutzaudit


Das als Teil eines umfassenderen Gesetzentwurfs vorgelegte Datenschutzauditgesetz (s. o. Nr. 2.2, vgl. auch 21. TB Nr. 2.4) folgt der Erkenntnis, dass durch die Förderung eines Datenschutzmanagements und die Schaffung wirtschaftlicher Anreize durch Zertifizierung Verstöße gegen datenschutzrechtliche Bestimmungen er schwert oder zumindest schneller offenbar werden. Auch wenn der vorgelegte Entwurf nur ein erster Schritt zu einer grundlegenden Modernisierung des Datenschutzes ist, enthält er doch eine Reihe positiver Aspekte.


Der Entwurf hat zu einer kontroversen datenschutzpolitischen Diskussion geführt. Dabei wurden berechtigte Bedenken geäußert, aber auch Befürchtungen, die nach meiner Ansicht nicht zutreffen.

In meiner Stellungnahme habe ich darauf hingewiesen, dass er eine Reihe positiver Ansätze enthält: Das Audit ist freiwillig. Durch wettbewerbliche Anreize ist es geeignet, ein höheres Datenschutzniveau zu erreichen, gewährleistet durch die Anwendung der Richtlinien die Vergleichbarkeit der zertifizierten Gegenstände und weist angesichts zahlreicher Veröffentlichungspflichten eine erfreuliche Transparenz auf.

Ich halte auf dieser Grundlage auch die für die Akzeptanz des Datenschutzaudits unabdingbare Qualitätssicherung für möglich. Allerdings besteht die Gefahr, dass dieser Anspruch in der Praxis nicht umfassend eingelöst werden kann. Zum einen ist die im Gesetzentwurf vorgesehene Kontrolldichte zu gering. Zum anderen muss damit gerechnet werden, dass die für die Aufsicht über die Kontrollstellen zuständigen Landesbehörden ihre Aufgaben wegen einer nicht ausreichenden Ausstattung nicht angemessen ausführen können. Dies gilt umso mehr, als die Konzeption des Audits mit einem nicht unerheblichen personellen und organisatorischen Aufwand für die Behörden verbunden ist.

Abzuwarten bleibt außerdem, inwieweit allein der Wettbewerb zwischen den Kontrollstellen tatsächlich zu einer hohen Qualitätssicherung führt und Gefälligkeitszertifizierungen wirksam vermieden werden können.

Darüber hinaus ist die vorgesehene Stellung des Datenschutzauditausschusses verbessert bedürftig, da er trotz der im Entwurf geregelter Unabhängigkeit einer sehr weitgehenden Rechtsaufsicht des BMI unterliegen soll.

Den gelegentlich geäußerten Vorwurf, die europarechtlich zwingend vorgesehene unabhängige staatliche Datenschutzaufsicht werde durch den Entwurf beschränkt oder gar ersetzt, teile ich nicht. Das geplante Datenschutzaudit soll neben die staatliche Datenschutzaufsicht treten und tange nicht. Sie ist ein zusätzliches Instrument der Datenschutzkontrolle, das ergänzend zur staatlichen Aufsicht bestehen soll.


2.5 Datenschutz und Outsourcing – Ein neuer Ansatz

Die Auslagerung von Aufgaben einschließlich der damit zusammenhängenden Erhebung und Verarbeitung personenbezogener Daten auf Dritte verlangt es, die Möglichkeiten und Grenzen des Outsourcing im Bundesdatenschutzgesetz klar zu regeln.

Sowohl öffentliche Stellen als auch Unternehmen erledigen viele Arbeiten nicht mehr selbst, sondern beauftragen in zunehmendem Umfang Dritte („Outsourcing“). Auch
die Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung ist von diesem Trend nicht ausge- nommen. Das Spektrum reicht dabei von einfachen Hilfs- tätigkeiten (z. B. Datenerfassung) über die Abwicklung umfangreicher Datenverarbeitungsprozesse (Rechenzentrum) bis hin zur weitgehend selbstständigen Wahrneh- mung von Aufgaben durch den Auftragnehmer (Kunden- betreuung bei Krankenkassen, Gehaltsbuchhaltung). Dass bei der Auslagerung von Aufgaben besonderer Wert auf den Datenschutz gelegt werden muss, belegen einige spektakuläre Vorfälle im Berichtszeitraum (vgl. u. a. Nr. 10.2.1, 10.2.2), in denen technische und organisatori- sche Schwachstellen bei beauftragten Dritten zu Daten- schutzzulagen führten.


Um auch hier ein bundesweit einheitliches Vorgehen zu gewährleisten, werden zurzeit durch die Unterarbeits- gruppe Empfehlungen ausgearbeitet, wie auch beim Outsourcing eine wirksame Datenschutzkontrolle ermög- lich werden kann. Wenn etwa eine Bundesbehörde einen privaten IT-Dienstleister beauftragt, gilt Folgendes:

Meine datenschutzrechtliche Kontrolle bei der Bundesbe- hörde erstreckt sich auch darauf, dass die in § 11 BDSG festgelegten Anforderungen eingehalten werden. Dafür ist sie mir gegenüber allein verantwortlich. Für die unmit- telbare Kontrolle beim IT-Dienstleister, also beim Auf- tragnehmer, ist primär die Datenschutzaufsichtsbehörde des Landes zuständig, in dem der Auftragnehmer seinen Sitz hat.


Kernausagen des Arbeitspapiers „Datenschutzrechtliche Grundlagen bei Auftragsdatenverarbeitung/ Outsourcing“:

1. Bedient sich eine öffentliche Stelle einer anderen öffentlichen oder nicht-öffentlichen Stelle zur rein technischen Abwicklung der Verarbeitung personenbezogener Daten, ist dies ein klassischer Fall der Auftragsdatenverarbei- tung i. S. v. § 11 BDSG. Dies bezieht sich ausschließlich auf solche Fälle, bei denen alle Verarbeitungsschritte nach einem vom Auftraggeber vorgegebenen Algorithmus ablaufen, also z. B.:
   - Auslagerung rechnertechnischer Vorgänge nach vorgegebenem Algorithmus auf externe Rechenzentren
   - Fernwartung
   - Entsorgung von Datenträgern
   - Technische Abwicklung einer virtuellen Poststelle

Eine über § 11 BDSG hinausgehende materiell-rechtliche Befugnis ist für diese Form des Outsourcings nicht erforderlich.

a) Die vollständige Verlagerung von Aufgaben auf eine andere öffentliche Stelle ist aufgrund Gesetzes oder eines Organisationserlasses möglich. Eine Übertragung auf eine nicht-öffentliche Stelle kann auf der Grundlage einer gesetzlichen Beleihung vorgenommen werden. Die damit einhergehende Übertragung der Datenverarbeitung ist als Datenübermittlung anzusehen; es handelt sich nicht um einen Fall der Datenverarbeitung im Auftrag. Beispiel:

- Abrechnung von Reisekosten oder Festsetzung von Dienstbezügen durch eine zentrale Stelle für Beschäftigte mehrerer Dienststellen

b) Bleibt die öffentliche Stelle Träger der Aufgabe und bedient sich lediglich für Teilaufgaben Dritter, muss zuerst die Zulässigkeit dieser teilweisen Aufgabenverlagerung geprüft werden. Bei der Ausgliederung hoheitlicher Aufgaben bedarf es eines gesetzlichen Übertragungssakes. Beispiele:

- Bearbeitung von Beihilfeangelegenheiten
- Privatisierung des Maßregelvollzugs

Bei sonstigen öffentlichen Aufgaben ist eine Übertragung auch auf vertraglicher Basis oder eine Unterstützung durch Verwaltungshelfer denkbar. Beispiele:

- Call-Center mit bloßer Weiterleitungsfunktion
- Inhaltliche Bearbeitung bei virtueller Poststelle

Bei der Verlagerung rein fiskalischer Tätigkeiten genügt in der Regel eine vertragliche Vereinbarung mit dem Auftragnehmer. Beispiel:

- Verwaltung von Liegenschaften


2.6 Outsourcing bei Trägern von Berufsgeheimnissen

Die von Ärzten, Rechtsanwälten, Steuerberatern oder anderen Berufsgeheimnisträgern eingesetzte Informations- und Kommunikationstechnik wird immer komplexer und aufwendiger: Eine Übertragung auf externe Dienstleister stößt auf datenschutzrechtliche Probleme.


Datenschutzrechtlich würde es genügen, die Auslagerung der rein technischen Vorgänge der Datenverarbeitung als klassische Form der Datenverarbeitung im Auftrag auf § 11 BDSG zu stützen (s. o. Nr. 2.5). Dies wird allerdings der besonderen rechtlichen Stellung der durch das Strafgesetzbuch (§ 203 StGB – s. Kasten zu Nr. 2.6) gesondert geschützten Berufsgeheimnisse, wie z. B. der ärztlichen Schweigepflicht, nicht gerecht. Anders als die datenschutzrechtlichen Anforderungen verpflichten die Berufsgeheimnisse nicht die für die Verarbeitung personenbezogener Daten verantwortliche Stelle, sondern den Träger des Berufsgeheimnisses persönlich, also beispielsweise...
den einzelnen Arzt oder Rechtsanwalt. Dieser darf die vom Berufsgeheimnis geschützten Informationen grundsätzlich nur dann gegenüber Dritten offenbaren, wenn der Betroffene eingewilligt (d. h. von der Schweigepflicht entbunden) hat oder eine gesetzliche Offenbarungsbefugnis existiert. § 11 BDSG ermöglicht zwar eine Verarbeitung personenbezogener Daten durch Dritte, enthält aber keine Offenbarungsbefugnis für die vom Berufsgeheimnis geschützten Informationen.


2.7 Projekt D115 – Einheitliche Behördenrufnummer

Bei der geplanten Einführung einer bundesweiten Behördenrufnummer sind schwierige datenschutzrechtliche Fragen zu lösen. Insbesondere muss gewährleistet werden, dass die von verschiedenen Behörden zu unterschiedlichen Zwecken geführten personenbezogenen Daten nicht zusammenggeführt werden. Auch in Deutschland soll eine bundesweit einheitliche Rufnummer – die „115“ – eingeführt werden, die sowohl

| § 203 Strafgesetzbuch |
| Verletzung von Privatgeheimnissen |
| (1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgemahnis, offenbart, das ihm als |

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilverfahren, der für die Berufsaufgaben, Beteiligung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung fordert,

2. Berufspychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, revidiertem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organ einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfung-, Buchprüfungs- oder Steuerberatungsgesellschaft,


5. staatlich anerkannten Sozialarbeiter oder staatlich anerkannten Sozialpädagogen oder

6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatrechtlichen, steuerberatlerischen oder verwaltungsrechten Verrechnungsstelle

anvertraut worden oder sonst bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2)…

Zentraler Baustein der Infrastruktur von D115 sind die kommunalen Service-Center, die von den Kommunen selbst oder in ihrem Auftrag von privaten Anbietern betrieben werden sollen. In einigen Regionen sind solche Service-Center bereits in Betrieb, wie z. B. das Call-Center Köln/Bonn/Leverkusen oder das Berlin Telefon 900. Diese regional begrenzten Lösungen sollen in das bundesweite Verfahren integriert werden.


Bei der geografischen Zuordnung der Anrufe an das örtliche Service-Center ist strikt darauf zu achten, dass nur die für die Zuordnung erforderlichen geografischen Angaben erhoben werden. Eine genaue adressencharfe Ortszuordnung der Anrufer muss auf jeden Fall unterbleiben. Die Projektleitung hat hierzu eine akzeptable Lösung entwickelt: Bei Anrufen aus dem Festnetz wird ausschließlich die Ortsnetzkennzahl, also die Vorwahl, genutzt. Bei Anrufen aus dem Mobilfunknetz werden die auf der Funkzelle basierende Standortinformation in eine Zielinformation (Amtlicher Gemeindeschlüssel oder Ortsnetzkennzahl) umgewandelt. Bei Anrufen aus internetbasierten Netzen soll eine geografische Zuordnung nicht vorgenommen werden. Damit ist sichergestellt, dass im Service-Center der genaue Aufenthaltsort der Anrufer nicht bekannt ist. Den größten Teil der Anrufe soll bereits im Service-Center („First Level“) beantwortet werden und zwar unabhängig davon, ob die Kommune, die das Service-Center betreibt, hierfür zuständig ist oder nicht. Um die Fragen sachkundig, schnell und korrekt beantworten zu können, sollen die Mitarbeitern der Service-Center eine Wissensdatenbank zur Verfügung stehen. Erst wenn sie die Fragen nicht beantworten können, etwa weil sie zu fachspezifisch sind oder ein konkretes Verwaltungsverfahren betreffen, wird der Anrufer an ein zentrales oder ressortspezifisches Service-Center eines Landes oder des Bundes oder ein anderes kommunales Service-Center weitergeleitet („Second Level“). Kann dem Anrufer auch hier nicht weitergeholfen werden, wird der Anruf an die zuständige Fachbehörde weitergegeben („Third Level“). Im Feinkonzept wird großer Wert darauf gelegt, dass in all diesen Fällen keine personenbezogenen Daten verarbeitet oder genutzt werden.

Neben der sofortigen Beantwortung oder der Weiterleitung der Anrufe sollen die Anliegen in elektronischer Form erfasst und an die jeweils zuständige Stelle weitergeleitet werden. Daher werden auch personenbezogene Daten erhoben und verarbeitet. Ich habe großen Wert darauf gelegt, dass in derartigen Fällen die ausdrückliche Einwilligung des Anrufers eingeholt wird. Ich halte hierfür eine mündliche Einwilligung für ausreichend, die nach § 4a BDSG aufgrund besonderer Umstände gemäß § 4a BDSG ausnahmsweise zulässig ist. Wichtig ist aber, dass sich die Anrufer eindeutig identifizieren und die Einwilligungen dokumentiert werden.

Sofern personenbezogene Daten zum Zwecke einer erneuten Auskunftserteilung oder der Weiterverfolgung eines Anliegens auf Wunsch der Anrufer gespeichert werden, erfolgt dies ausschließlich lokal im jeweiligen Service-Center. Die Daten sind zu löschen, wenn sie nicht mehr erforderlich sind. Auf meine Empfehlung wurde die maximale Speicherdauer nach abschließender Bearbeitung auf drei Monate begrenzt. Während der Test- und Pilotphase ist zu prüfen, inwieweit die Verkürzung möglich ist.

Falls eine Kommune das Service-Center nicht selbst betreibt, sondern hiermit ein privates Unternehmen beauftragt, sind weitere Anforderungen zu beachten. So muss zunächst geprüft werden, in welchem Umfang und auf welcher Grundlage eine Verarbeitung überhaupt möglich ist, ohne dass dabei datenschutzrechtliche Belange beeinträchtigt werden (zu den Anforderungen bei der Auftragsdatenverarbeitung s. Nr. 2.5).


Ich werde das Projekt D115 weiterhin intensiv begleiten.
2.8 Datenschutz – bloß unnötige Bürokratie?


- Hinweisrichtung nach § 4a Absatz 1 Satz 2 BDSG

- Unterrichtungspflicht, Unterrichtung des betrieblichen Datenschutzbeauftragten nach § 4g BDSG
  Fast 50 Mio. Euro soll die Umsetzung dieser Pflicht kosten, die es den betrieblichen Datenschutzbeauftrag-
ten ermöglicht, sich einen Überblick über die Datenverarbeitung in ihrem Betrieb zu verschaffen und dementsprechend zu beraten, Mitarbeiter zu schulen und Missbräuchen vorzubeugen.

Werbewiderspruch nach § 28 Absatz 4 Satz 2 BDSG


Dieses Verfahren ist jedoch standardisiert. Die Betroffenen werden nicht individuell angesprochen.


Ich hoffe, dass dieses Arbeitspapier, das ausdrücklich zu Kommentierung und Stellungnahme auffordert, weitere Diskussionen anstößig und dazu beiträgt, die vielfach noch unbefriedigende Situation zu verbessern, und – soweit nötig – auch zu gesetzlichen Präzisierungen führt.
Kasten zu Nr. 2.9

Beispiele für Konfliktsituationen:

- Auskunftsanspruch gegenüber der Schule:
  - Können Schülerinnen und Schüler den Anspruch eigenständig geltend machen und ab welchem Alter?
  - Kann ihnen entgegengehalten werden, ihre Eltern hätten bereits Auskunft erhalten?
  - Haben die Eltern einen Anspruch auf Auskunft, auch wenn der betroffene Jugendliche dies ausdrücklich nicht wünscht?

- Einwilligung in die Veröffentlichung von Fotos:
  - Bedarf es der Einwilligung sowohl der Eltern als auch des Jugendlichen?
  - Können die Eltern gegen den ausdrücklichen Willen des Jugendlichen wirksam einwilligen?
  - Kann umgekehrt der Jugendliche gegen den ausdrücklichen Willen der Eltern wirksam einwilligen?

- Einwilligung in die Verarbeitung personenbezogener Daten zu Werbezwecken:
  - Reicht die Einwilligung des Jugendlichen und gegebenenfalls ab welchem Alter?
  - Können die Eltern gegen den Willen des betroffenen Jugendlichen einwilligen?
  - Wem steht das Widerrufsrecht zu?

3 Wirtschaft

3.1 Gibt es eine Balance zwischen informationeller Selbstbestimmung und wirtschaftlichen Interessen?


Für mich ist es vor diesem Hintergrund keine Frage, dass der Staat hier die Bürgerinnen und Bürger schützen muss. Auch der Präsident des Bundesverfassungsgerichts, Professor Dr. Papier, sieht den Staat in der Pflicht, ein „angemessenes Schutzregime“ zu schaffen. Noch sehe ich hier ein erhebliches Defizit. Der Staat hat zwar bei den Sicherheitsgesetzen erheblich aufgerüstet, der Datenschutz in der Privatwirtschaft und vor allem die Frage, wie die Bürgerinnen und Bürger vor zu viel Datensammlerwut in der Wirtschaft geschützt werden können, ist in der Vergangenheit häufig vernachlässigt worden. Obwohl die als Reaktion auf aktuelle Missstände initiierten Gesetzesinitiativen durchaus zu begrüßen sind, können punktuelle Verbesserungen eine grundlegende Anpassung des Datenschutzrechts an die modernen Formen der Datenverarbeitung nicht ersetzen (s. u. Nr. 3.4.4 und Nr. 3.4.5).

Eine demokratische Informationsgesellschaft ist ohne eine Ethik der Selbstbegrenzung nicht denkbar: Nicht alles was möglich ist, darf auch gemacht werden. Informationen sind nicht das Maß aller Dinge, sonst wird der Mensch zum bloßen Objekt der Information, während die Information, das einzelne Datum zum objektiven, unbe stechlichen Wert erhoben wird, dem der einzelne Mensch in seiner Subjektivität und Fehlbarkeit nichts mehr entgegensetzen kann.

3.2 Telekommunikations- und Teledienste

3.2.1 Vorratsdatenspeicherung: Das Bundes-verfassungsgericht hat das letzte Wort

Die zum 1. Januar 2008 in Kraft getretene gesetzliche Verpflichtung zur Vorratsdatenspeicherung musste sogleich auf den Prüfstand des Bundesverfassungsgerichts (s. Kasten zu Nr. 3.2.1).

Bereits in meinem 21. TB (Nr. 10.1) hatte ich über die EG-Richtlinie zur Vorratsdatenspeicherung (RL 2006/24/EG vom 15. März 2006) berichtet. Parallel zur mittlerweile erfolgten Verabschiedung des die Richtlinie umsetzenden Gesetzes hat es massive öffentliche Kritik gegeben. So wurden gleich mehrere Beschwerden beim Bundesverfassungsgericht eingereicht, unter ihnen eine „Massenverfassungsbeschwerde“, an der sich ca. 34.000 Bürgerinnen und Bürger beteiligten.

Kasten zu Nr. 3.2.1

Vorratsdatenspeicherung

sierung erfolgen. Auch unabhängig von den Inhaltsdaten der Telekommunikation können umfassende Persönlichkeitsbilder, Soziogramme und Bewegungsprofile erstellt werden, die über verschiedene Lebensbereiche Auskunft geben können. Nicht vergessen werden darf darüber hinaus, dass das Risiko sowohl des vorsätzlichen Missbrauchs aber auch das fahrlässiger Datenschutzverstöße mit zunehmender Quantität der Datenbestände stetig steigt. Das zeigen auch die jüngsten Fälle, vor allem aus dem Bereich der Telekommunikation.

Mit Blick auf die Verwendung der auf Vorrat gespeicherten Daten habe ich vor allem die unangemessen niedrig gehaltene Zugriffschwelle des § 100 g StPO für Strafverfolgungsbehörden kritisiert. Obwohl die Richtlinie als Zweck der Vorratsdatenspeicherung nur die Verfolgung von schweren Straftaten nennt, erlaubt § 100 g StPO die Abfrage von Verkehrsdaten bereits zur Verfolgung von Straftaten von erheblicher Bedeutung oder sogar von nicht erheblichen Straftaten, sofern diese mittels Telekommunikation begangen wurden (s. auch Nr. 5.1).


Wenngleich auch die Hauptsacheentscheidung des BVerfG noch aussteht, hat es mit zwei Eibeschlüssen im Frühjahr und Herbst 2008 zwar nicht die Vorratsdatenspeicherung als solche untersagt, den Strafverfolgern, den bayerischen und thüringischen Landespolizeien und dem bayerischen Verfassungsschutz beim Zugriff auf die Vorratsdaten aber bereits vorläufig deutliche Beschränkungen auferlegt. In der Entscheidung vom 11. März 2008 (1 BvR 256/08) wurde die Verwendung der gespeicherten Daten durch die Strafverfolgungsbehörden nur unter engen Voraussetzungen für zulässig erklärt. So dürfen die Vorratsdaten nur dann an die Strafverfolgungsbehörden übermittelt werden, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat im Sinne des § 100a Absatz 2 StPO ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich er schwert oder aussergewöhnlich wäre (§ 100a Absatz 1 StPO). Die Auskunftserteilung wurde damit – wenn auch nur vorläufig – erheblich eingeschränkt. Diese Linie wurde mit einem weiteren Beschluss vom 28. Oktober 2008 (1 BvR 256/08) bestätigt. Für den Abruf von Daten zur Gefahrenabwehr durch die Polizei in Bayern und Thüringen muss demnach eine dringende Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes vorliegen oder aber eine gemeinsame Gefahr drohen. Im Falle eines Abrufs durch den Verfassungsschutz müssen zugleich die Vor aussetzungen der §§ 1 Absatz 1 und § 3 des Artikel-10-Ge setzes vorliegen. In jedem Fall gilt zudem der Grundsatz, dass die abgefragten Vorratsdaten nicht für weitere Zwecke verwendet werden dürfen.

Mit den beiden Beschlüssen hat das BVerfG einen wichtigen, aber aus prozessrechtlichen Gründen noch nicht abschließenden ersten Schritt getan. Die Hauptsacheentscheidung bleibt aber abzuwarten.

### 3.2.2 Fall Telekom/Lehren aus dem Missbrauch von Verkehrsdaten bei der Telekom

**Der Missbrauch von Verkehrsdaten bei der Deutschen Telekom AG (DTAG) verdeutlicht, dass die Stellung der betrieblichen Datenschutzbeauftragten gestärkt, ihre Personalausstattung verbessert und die Kooperation zwischen Datenschutz und Daten verarbeitenden Stellen im Unternehmen intensiviert werden muss.**


unter Strafandrohung von maximal fünf Jahren Freiheits-
strafe gestellt. Die Staatsanwaltschaft Bonn ermittelte seit
Mitte letzten Jahres mit Unterstützung des Bundeskrimi-
nalams in einem sehr umfangreichen Verfahren zu den
Vorgängen bei der DTAG, das bei Redaktionsschluss
noch nicht abgeschlossen war.

Die Feststellung individueller Verstöße gegen strafrechtli-
che Normen und die Entscheidung über die Anklageher-
bung ist Aufgabe der Strafverfolgung. Demgegenüber ist
die Aufgabe des Datenschutzes eher präventiver und zu-
kunftsgerechter Art. Wegen der laufenden Ermittlungen
der Staatsanwaltschaft Bonn habe ich meine Prüfungstä-
tigkeit bei der DTAG darauf konzentriert, die Abläufe
und die datenschutzrechtlichen Risiken bei der Verarbei-
tung von Verkehrsdaten zu analysieren, um auf eine Re-
duzierung der Risiken hinzuwirken.

Die Verarbeitung von Verkehrsdaten des Festnetzes er-
folgt nicht zentralisiert, sondern dezentral an zahlreichen
Standorten der DTAG. Erste Aufgabe bei meinen Kon-
trollen in Bonn war es deshalb, einen groben Überblick
über die Strukturen und Abläufe bei der Verarbeitung von
Verkehrsdaten zu gewinnen. Dieser Überblick musste ge-
meinsam mit den beteiligten Stellen und den Mitarbeitern
des Konzernschutzes erarbeitet werden. Aufgrund
der Vielzahl der Systeme und der verteilten Zuständigkei-
ten bei der DTAG war es teilweise sehr mühsam, die not-
wendigen Struktur- und Prozessinformationen zur Verar-
beitung von Verkehrsdaten, zum Rechtemanagement und
zur Protokollierung zu erhalten. Auch beim Konzernda-
tenschutz bestand zu Anfang meiner Kontrolle noch kein
vollständiger Überblick.

Der Zugriff auf Verkehrsdaten ist für betriebliche Zwe-
cke, nämlich insbesondere für die Abrechnung gegenüber
dem Kunden, aber auch gegenüber anderen Telekommunika-
tionsunternehmen, ferner zur rechtzeitigen Erken-
nung von Störungen und Missbrauchsfällen erforderlich.
Ein missbräuchliches „Abziehen“ oder Kopieren von
Verkehrsdaten kann also an mehreren Punkten ansetzen.
Im Interesse optimierter Prävention müssen deshalb alle
„risikogeneigten“ Datenverarbeitungen analysiert und be-
wertet werden.

Als wesentliches Ergebnis meiner Prüfungen hinsichtli-
cher der Verarbeitung von Verkehrsdaten im Festnetzbereich
lässt sich festhalten:

Die Daten werden mehrfach an verschiedenen Stellen ge-
speichert. Die Verkehrsdaten zu einem Gespräch können
je nach Konstellation mehrfach vollständig und zusätzlich
mit verkürzter Zielrufnummer erfasst werden. Dabei wer-
den für die Missbrauchserkennung sogar Daten der An-
rufversuche erhoben. Mit Blick auf das gesetzliche Gebot
der Datensparsamkeit (§ 3a BDSG) sollte hier eine deutli-
che Reduzierung erfolgen, auch um Missbrauchsmöglich-
keiten und Täteleigenschaften zu verringern.

Verkehrsdaten werden teils auch zu lange gespeichert.
Hier muss einerseits im Unternehmen die Speicherdauer
an verschiedenen Stellen überprüft und reduziert werden.
Andererseits sollte auch der Gesetzgeber sich dieser The-
matic annehmen. Während die Speicherdauer und der
Umfang der Daten für Zwecke der Abrechnung mit dem
Kunden und bei der Vorratsdatenspeicherung minutiös
geregt sind, fehlen entsprechend klare Regelungen für
andere Verwendungen von Verkehrsdaten.

Die DTAG hat auf meine Aufforderung damit begonnen,
die erteilten Zugriffsberechtigungen zu überprüfen. Für eine An-
wendung, mit der nur in besonderen Fällen auf Verkehrs-
daten zugegriffen wird, waren allein fast 4 000 Nutzer re-
gistriert. Auch wenn zur Gewährleistung eines effizienten
Service die Erforderlichkeit von Zugriffsmöglichkeiten
für eine nicht geringe Zahl unternehmensinterner Nutzer
grundsätzlich plausibel erscheint, bedarf es zur Minde-
runz von Missbrauchsrisiken gleichwohl einer Überprü-
fung und Aktualisierung mit dem Ziel einer Reduzierung
von Zugriffsmöglichkeiten. Die „Rechtshistorie“, also die
Dokumentation der Zuweisung von Zugriffsberechtigungen
einer Mitarbeiter auf bestimmte Anwendungen und Sys-
terne, muss zudem sicher dokumentiert werden.

Die revisions-, also manipulationssichere Protokollierung
von Zugriffen auf sensible Daten gehört zu den essenti-
eln Forderungen des Datenschutzes. Aus der Protokollie-
rung muss erkennbar sein, ob der Zugriff durch einen Ad-
ministrator, sonstige Mitarbeiter der DTAG oder externe
Kräfte erfolgt ist. Die datenschutzrechtliche Kontrolle
sollte durch zentrale Zugriffsmöglichkeiten (selbstver-
ständlich in einem streng kontrollierten Verfahren) er-
leichtert werden.

Ein Teil der Missbrauchserkennungssysteme wurde von
Mitarbeitern aus dem Bereich der Konzernsicherheit
dient. Hier bestand technisch die Möglichkeit, Ver-
kehrsdaten zu erheben. Konzernsicherheit und Miss-
brauchserkennung sind zur Risikominimierung deutlich
durchzuführen. Aufträge an die Konzernsicherheit sind
zudem präzise und nachvollziehbar zu erteilen und zu do-
kumentieren. Der Konzernschutz muss bei „daten-
schutzsensiblen“ Maßnahmen der Konzernsicherheit
frühzeitig und vor dem Zugriff auf Datenbestände betei-
ligt werden.

Das BDSG verpflichtet die Daten verarbeitenden Stellen
zur Information und Unterstützung des betrieblichen bzw.
behördlichen Datenschutzbeauftragten, damit dieser seine
gesetzliche Informations- und Kontrollaufgabe wirksam
erfüllen kann. Letztendlich bestand beim Konzerndaten-
schutz der DTAG jedoch kein vollständiger und ausrei-
chend detaillierter Überblick über die Systeme zur Daten-
verarbeitung. Dieser Umstand war schließlich Grund
einer Beanstandung.

Die DTAG hat seit Juni 2008 einiges aufgeholt, um ähnli-
che Vorfälle für die Zukunft so weit als möglich auszu-
schließen. Aus der Vielzahl der Maßnahmen möchte ich
hier nur einzelne herausheben:

- Die Aufwertung der zentralen Aufgabe „Datenschutz“
  wird mit der Einrichtung des neuen Vorstandes für Recht
  und Datenschutz und der bereits 2008 eingeleiteten Per-
  sonalverstärkung deutlich. Ermittlungsaufträge für die
  Konzernsicherheit sollen künftig kritisch geprüft und
  nachvollziehbar dokumentiert werden, um die Abwei-
  gung und den Missbrauch sensibler Daten auszuschlie-
  ßen. Die Analyse und Behebung datenschutzrechtlicher
Schwachstellen bleibt angesichts der dislozierten Datenverarbeitung aber eine Daueraufgabe.


Die aktuellen Vorgänge werfen Fragen jenseits der Verantwortlichkeit des einzelnen Unternehmens auf. Auch wenn es keine Kausalität zwischen den Vorgängen bei der DTAG und der erst nach diesen eingeführten Vorratsdatenspeicherung (s. Nr. 3.2.1) gibt, liegt doch die Frage nahe, ob sich mit der Vorratsdatenspeicherung das Missbrauchsrisiko nicht weiter erhöht. Die Forderung nach Datenminimierung zwecks Missbrauchsrisikominimierung bleibt deshalb unverändert aktuell.

Der „Fall Telekom“ gibt über den Einzelfall hinaus Anlass, eine präzisere Regelung der Befugnisse von Telekommunikationsunternehmen bei der Eingrenzung von Störungen und bei der Missbrauchserkennung zur Diskussion zu stellen. Die gegenwärtigen Regelungen in § 100 Absatz 1 und 3 TKG sind sehr knapp und zumindest „interpretationsfähig“. Eine ausdrückliche und präzise Auslegung ist zu wünschen. Die gegenwärtigen Regelungen in § 100 Absatz 1 und 3 TKG sind nicht ausreichend.

Umfrage zeigt, dass die Anbieter sich vielfach um einen höheren Datenschutzstandard bemühen, gleichwohl ein beträchtlicher Optimierungsbedarf besteht. Eine datenschutzgerechte Ausgestaltung der Auftragsdatenverarbeitung (vgl. Nr. 2.5) durch Call-Center kann durch Einbeziehung des TK-Anbieters dadurch erreicht werden. Ich werde die TK-Anbieter daher über meine Forderungen in Kenntnis setzen und die Umsetzung dieser konkreten Maßnahmen überprüfen.

### 3.2.3 Datenschutzgerechte Ausgestaltung der Auftragsdatenverarbeitung in Call-Centern

Eine Umfrage unter verschiedenen Telekommunikationsdienstanbietern (TK-Anbietern) zeigt, dass bei der Auftragsdatenverarbeitung durch Call-Center der Datenschutz vielfach eine zu geringe Rolle spielt.

Ob Änderung des Handy-Vertrags oder technische Probleme mit dem Internet-Zugang – Call-Center sind heutzutage für Kunden wie TK-Anbieter aus dem täglichen Leben nicht mehr wegzudenken. Um so schlimmer ist es, dass der Missbrauch von personenbezogenen Daten, wie Name, Adresse, Telefonnummer oder gar Bankverbindung, in Call-Centern immer wieder ein aktuelles Thema ist. Aus diesem Grund habe ich verschiedene TK-Anbieter gebeten, ihre Rahmenverträge mit den von ihnen beauftragten Call-Centern vorzulegen. Das Ergebnis dieser Umfrage zeigt, dass die Anbieter sich vielfach um einen höheren Datenschutzstandard bemühen, gleichwohl ein beträchtlicher Optimierungsbedarf besteht. Eine datenschutzgerechtere Ausgestaltung der Auftragsdatenverarbeitung (vgl. Nr. 2.5) durch Call-Center kann durch Einbeziehung des TK-Anbieters ein zeitlich und räumlich uneingeschränktes Kontrollrecht eingeräumt werden. Ferner ist vertraglich sicherzustellen, dass der BIDT die Datenverarbeitung, für die der TK-Anbieter verantwortlich ist, bei Call-Center uneingeschränkt kontrollieren kann.

Über die Einhaltung dieser Bestimmungen muss ein sachkundiger Datenschutzbeauftragter des Call-Centers wachen. Zudem muss dem Datenschutzbeauftragten des TK-Anbieters ein zeitlich und räumlich uneingeschränktes Kontrollrecht eingeräumt werden. Ferner ist vertraglich sicherzustellen, dass der BIDT die Datenverarbeitung, für die der TK-Anbieter verantwortlich ist, bei Call-Center uneingeschränkt kontrollieren kann.

Sollten Verstöße gegen das Datenschutzrecht festgestellt werden, so sind die Datenschutzbeauftragten des Call-Centers sowie des TK-Anbieters unverzüglich darüber zu informieren. Verstöße sollten mit Vertragsstrafen sanktioniert werden.
3.2.4 Nicht jeder will, doch mancher kommt auch gegen seinen Willen in das Telefonbuch

Immer wieder beklagen Telefonteilnehmer, gegen ihren Willen in öffentliche Verzeichnisse eingetragen zu werden.

öffentliche Kundenverzeichnisse, also gedruckte und elektronische Telefonbücher, die telefonische und die „Internet-Auskunft“, werden häufig gerne genutzt. Viele Telefonteilnehmer wollen so auch erreichbar sein – aber eben nicht alle. Oftmals gibt es gute Gründe, die Rufnummer und/oder Adresse nicht publik werden zu lassen. Gleichwohl ist häufig festzustellen, dass Daten gegen den erklärten Willen des Anschlussinhabers veröffentlicht werden.

Bei den Betroffenen, die sich wegen eines ungewollten Eintrags ihrer Daten an mich gewandt haben, handelte es sich – wie bereits im Berichtszeitraum meines TB (Nr. 11.12) – im Wesentlichen um Kunden der Deutschen Telekom AG (DTAG). Darunter waren auch mehrere Polizeibeamte, die im sicherheitskritischen Bereich tätig sind. Durch den ungewollten Eintrag mit Rufnummer und Anschrift sahen sie ihre eigene Sicherheit sowie die ihrer Familie gefährdet. In einem Fall wurde die DTAG mit einer nicht unerheblichen Schadensersatzforderung konfrontiert, da ein nicht zu vermeidender Umzug im Raum stand.


3.2.5 Bonitätsprüfung bei neuen Telefonkunden

Bei der Entscheidung über den Abschluss von Handy-Verträgen nutzen die Telekommunikationsunternehmen Informationen über die tatsächliche oder angenommene Zahlungsfähigkeit der Kunden, die sie bei Auskunftanfragen abfragen. Die Entscheidung erfolgt oftmals (weitgehend) automatisiert. Für den Interessenten ist dieses Verfahren vielfach nicht nachzuvollziehen.

Im Rahmen einer schriftlich durchgeführten datenschutzrechtlichen Prüfung bei 23 Telekommunikationsdienstanbietern habe ich festgestellt, dass wichtige Vorgaben des BDSG bei einem nicht unerheblichen Anteil der Unternehmen nicht beachtet wurden. Die Antworten ergaben im Wesentlichen folgende Defizite:

1. Häufig wurden die Interessenten bei Vertragsablehnung an die Wirtschaftsauskunft verwiesen, die entsprechende Negativmerkmale oder einen schlechten Score-Wert übermittelte, ohne sich mit den Argumenten des Betroffenen auseinander zu setzen. Dies entspricht weder dem Wortlaut noch der Intention des BDSG. Automatisierte Einzelentscheidungen, die zur Ablehnung eines Antrages auf Abschluss eines Telekommunikationsvertrages führen, sind nur unter den Voraussetzungen von § 6a Absatz 2 Nummer 2 BDSG zulässig. Danach muss die Wahrung des berechtigten Interesses des Betroffenen durch geeignete Maßnahmen gewährleistet werden, z. B. durch die Möglichkeit, sich noch einmal an die verantwortliche Stelle zu wenden, um seinen Standpunkt geltend zu machen. Dazu muss dem Betroffenen mitgeteilt werden, dass überhaupt eine automatisierte Ablehnung erfolgt ist. Die verantwortliche Stelle ist dann verpflichtet, ihre Entscheidung erneut zu prüfen. Einem abgelehnten Antragsteller muss also mitgeteilt werden, wie und an wen er sich in dem entsprechenden Unternehmen wenden kann. Dabei muss es sich um Mitarbeiter handeln,
die über entsprechende Kompetenzen verfügen, um die Darstellung der Betroffenen bewerten zu können, damit die vom Gesetz geforderte erneute Prüfung durchgeführt werden kann.


Im Zuge der weiteren Erörterungen habe ich die betroffenen Telekommunikationsunternehmen aufgefordert, die erforderlichen Verfahrensänderungen vorzunehmen. Die betroffenen Unternehmen haben mir zugesichert, meine Rechtsauflösung zum Umgang mit Bonitätsdaten künftig zu beachten.

3.3 Postunternehmen

3.3.1 Anlasslose Weitergabe von Sendungsdaten in die USA


Es bleibt festzuhalten, dass seit Inkrafttreten des „Trade Act of 2002“ die US-Zollbehörden bei der Warneinfuhr...
keine zusätzlichen Daten zu einer Sendung verlangen, sondern lediglich eine neue – elektronische – Form der Aufbereitung vornehmen. Elektronisch vorliegende Da-
ten können jedoch zweifellos einfacher aufbewahrt, aus-
gewertet und – ggf. auch für andere Zwecke – genutzt
werden. Ebenso sehe ich die Speicherdauer von sechs Jahren kritisch. Da die USA in der Gestaltung ihrer Einfuhrbestimmungen frei sind, ist dies eine zwar uner-
freuliche, aber von europäischer Seite wohl kaum aufzu-
haltende Entwicklung. Die Erweiterung der Meldepflicht &
Speicherung der sendungsbezogenen Daten auch auf
Briefe – wie im „Trade Act of 2002“ prinzipiell vorgese-
hen – hielt ich für besonders problematisch. Deshalb er-
warte ich von der Bundesregierung und den EU-Institu-
tionen, weiterhin auf den Verzicht einer derartigen
Ausweitung der elektronischen Erfassung hinzuwirken.

Auch die Europäische Kommission strebt die Ablösung
der papierbasierten Zollabwicklung durch ein elektroni-
sches System an. Daher arbeitet die Deutsche Post AG
zusammen mit anderen Postunternehmen an einem Ver-
fahren zum elektronischen Austausch zollrelevanten Da-
ten (MEDICI – Mails Electronic Data Interchange &
Cutoms Integration). Die Umstellung auf ein elektroni-
sches Verfahren darf aber nicht zu einer verlängerten
Speicherung von Daten führen.

3.3.2 Prüfungen bei Postunternehmen –
Einzelfälle meiner Kontrolltätigkeit

Die Öffnung des Briefmarkts für private Anbieter brachte
nicht nur mehr Wettbewerb, sondern auch mehr Be-
swerden über Datenschutzverstöße.

Zum Ende des Jahres 2007 lief die vom Gesetzgeber der
Deutschen Post AG eingeräumte Exklusivlizenz aus:
Schon lange hatten sich Hunderte lizenzierte Wettbewer-
ber auf die Öffnung des milliardenschweren Briefmarkts
vorbereitet. Doch nicht immer gingen die Umstrukturie-
rungen vom kleinen Postdienstleister zum konkurrenzfä-
Hörde wenden.

Auch im Zuge der Expansion der PIN AG kam es im Un-
ternehmen zu datenschutzrechtlichen Defiziten. Viele
Petenten beschwerten sich über eine mangelhafte Zettel-
ungssicherheit. Um diese Eingaben sachgerecht beantwor-
ten zu können, bin ich auf die Zusammenarbeit mit den
Unternehmen angewiesen. Unso ärgerlicher war es, dass
meine Anfragen unbeantwortet blieben. Folglich konnte
ich den Petenten nicht in angemessener Zeit weiterhelfen.

Diesen Prozess werde ich durch regelmäßige Kontrollen
und Beratungsgespräche begleiten.

Zahlreiche Kontrollbesuche bei Kurier-, Paket- sowie
Briefdiensten zeigen, dass viele Postdienstleister ihr Ge-
schäft grundsätzlich datenschutzgerecht betreiben. So
habe ich im Berichtszeitraum den Briefdienst des Logis-
tikkonzerns Thomas Nationwide Transport (TNT)
TNT Post kontrolliert. Der betriebliche Ablauf ist so or-
ganisiert, dass datenschutzrechtlich relevante Vorschrif-
ten eingehalten werden. Das Qualitätsmanagement bindet
den Datenschutz ein und sorgt für seine Einhaltung und
Fortentwicklung. Gleiches gilt auch auf die Beförderung
von Waren- und Expresssendungen durch den Paketdienst
TNT Express.

Immer wieder erreichen mich Bürgeranfragen, woher der
Absender die Anschrift bezogen hat. Hier muss man zwei
wesentliche Aspekte unterscheiden: Zum einen befördern
Postdienstleister Sendungen, die mit Anschriften aus dem
Adressehandel beschriftet wurden, insbesondere bei Wer-
besendungen. Das Postunternehmen beschränkt sich auf
das Einsammeln, Befördern und Zustellen der Sendun-
gen. In diesem Falle müssen sich die Petenten direkt an
den Absender bzw. die für diesen zuständige Aufsichtsbe-
hörde wenden.

Zum anderen darf ein Postdienstleister im Adressehandel
selber tätig sein, solange er die Daten für sein Geschäft
nicht aus seiner Tätigkeit als Postdienstleister bezieht.

Recht komplex stellt sich diese Materie bei der Deutschen
Post AG und ihren rechtlich selbständigen Tochtergesell-
schaften Deutsche Post Adress GmbH und Deutsche Post
Direkt GmbH dar, da die Posttöchter nicht nur eigene Da-
ten, sondern auch Daten aus Nachsendeaufrägen im Auf-
trag der Deutschen Post AG verarbeiten. Während die da-
tenschutzgerechte Erhebung, Speicherung und Nutzung
der Daten aus Nachsendeaufrägen unter meine Aufsicht
fällt, obliegt die datenschutzrechtliche Prüfung der Da-
tenverarbeitung durch die Posttöchter der Aufsichtsbe-
hörde für den nicht-öffentlichen Bereich, hier der Landes-
beauftragten für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen (LDI NRW). Ebenso ist die Zustän-
digkeit für die Deutsche Post AG außerhalb der Post-
dienstleistungen mit Wegfall des Postmonopols zum
1. Januar 2008 auf die LDI übergegangen. Bei der daten-
schutzrechtlichen Kontrolle der Anschriftenweitergabe
arbeitet ich mit der LDI intensiv zusammen. Datenschutz-
rechtliche Verstöße oder einen kritischen Umgang mit
daten konnte ich bei gemeinsamen Kontrollen nicht fest-
stellen.

3.4 Wirtschaft allgemein

3.4.1 Die Europäische Dienstleistungs-
richtlinie und das Binnenmarktinfoma-
tionssystem IMI

Die Umsetzung der Europäischen Dienstleistungsricht-
linie muss bis Ende 2009 abgeschlossen sein – daten-
schutzrechtliche Aspekte verdienen mehr Aufmerksam-
keit.

In Artikel 43 der EU-DLRL wird zwar darauf hingewiesen, dass die Vorschriften zum Schutz personenbezogener Daten eingehalten werden müssen, diese jedoch auf nationaler Ebene definiert werden. Insbesondere sind der Übermittlungsumfang, die Empfänger der Daten, die Speicherdauer und die Löschungs-/Tilgungsregelungen, die Auskunfts- und Änderungsrechte von Betroffenen sowie die datenschutzrechtliche Kontrolle zu konkretisieren.


<table>
<thead>
<tr>
<th>Binnenmarktinformationssystem IMI</th>
</tr>
</thead>
</table>


Die Artikel-29-Gruppe der europäischen Datenschutzbehörden hat zu den Datenschutzaspekten des IMI Stellung genommen (Stellungnahme Nr. 7/2007, WP 140). Die Gruppe schlägt vor, für den Datenaustausch innerhalb des


Vor dem Hintergrund dieses getroffenen Kompromisses bin ich mir mit meinen Länderkollegen einig, dass hier Bundes- und Landesgesetzgeber gefordert sind, kurzfristig Anpassungen in den einschlägigen Fachgesetzen vorzunehmen.

3.4.2 Neuer Energieausweis führt zu Ärger bei Hauseigentümern


3.4.3 Die neue Publizitätspflicht im elektronischen Unternehmensregister und E-Bundesanzeiger

sellschaft mbH als Betreiberin des elektronischen Bun-
desanzeigers eingereicht werden. Der Kreis der offene-
gungspflichtigen Unternehmen sowie Art und Umfang der
einzureichenden Unterlagen sind hingegen unverän-
derth verblieben.

Hierzu haben mich viele Eingaben von Unternehmen er-
reicht, die mit der Veröfentlichen ihrer Unternehmensdaten
über die Internet-Plattformen www.unternehmensregister.de
und www.ebundesanzeiger.de nicht einverstanden waren.
Der freie Zugang für jedermann ist jedoch datenschutz-
rechtlich nicht zu beanstanden. Die Angaben über juristi-
sche Personen und Personennahme haben der Gesetzge-
ber aus dem Anwendungsbereich des BDSG bewusst
ausgenommen. Während für den Einzelnen die informa-
tionselle Selbstbestimmung den Ausgangspunkt bildet, un-
terliegen juristische Personen insbesondere aus Gründen
des Verbraucher-, Anleger- und Gläubigerschutzes vie-
fältigen Pflichten zur Publizität und Rechnungslegung.
Datenschutzregeln sind auf derartige Regeln – zumindest
nach deutschem Recht – nicht anwendbar.

Durch einige Eingaben bin ich darauf hingewiesen wor-
den, dass bei der Suche z. B. nach einem Namen eines
Wirtschaftsprüfers oder Steuerberaters nicht nur die von
ihm zu publizierenden Unternehmensdaten, sondern auch
die aller Unternehmen als Suchergebnis angezeigt wur-
den, bei denen er in seiner Funktion als Wirtschaftsprüfer
oder Steuerberater mitgewirkt hat. Das Bundesministe-
rerin der Justiz hat inzwischen die Bundesaufzücker
Verlagsgesellschaft mbH angewiesen, diese Volltextsuche
in den Jahresabschlüssen so abzuschalten, dass lediglich
noch den Firmenbezeichnungen der veröffentlichen-
den Unternehmen bzw. nach Teilen hiervon recherchiert
werden kann. Seit August 2008 ist der Suchmodus beider
Plattformen entsprechend angepasst worden.

3.4.4 Der Mensch ist kein Score-Wert

Bereits in meinen zurückliegenden Tätigkeitsberichten
habe ich auf die Gefahren der Profilbildung hingewiesen
und ein gesetzesgebendes Handeln angemahnt (vgl.
20. TB Nr. 11.4 ff.; 21. TB Nr. 9 ff.). Den nun im Berichts-
zeitraum vorgelegten Gesetzentwurf (Bundestagsdruck-
sache 16/10529), der die Tätigkeit von Auskunftso-
regeln und Score-Verfahren transparenter machen will,
beprüfte ich. Ich wünsche mir jedoch ein klareres Be-
kenntnis zum Schutz des Einzelnen vor einer auseinander-
fallenden Profilbildung.

Der Entwurf der Bundesregierung sieht eine ausdrückli-
che Rechtsgrundlage für die Einmeldung von personen-
bezogenen Daten in ein Auskunfteisystem vor. Dabei
handelt es sich um Daten über nicht-vertragsgemäßes
Verhalten. Hiervon gibt es zwei wichtige Ausnahmen:
Kreditinstitute dürfen auch Daten über die Begründung,
ordnungsgemäße Durchführung und Beendigung eines
Vertragsverhältnisses an eine Auskunftso weitergeben.
Zudem bleibt es einem Unternehmen unbenommen, im
Wege einer Einwilligung vom Betroffenen die Erlaubnis
to erhalten, weitere Daten an eine Auskunftso zu übermit-
teln. Der Gesetzentwurf regelt zudem die Durchführung
von Scoring-Verfahren und verschärft das Auskunftsrecht
der Betroffenen: So müssen alle Auskunfto zukünftig
einmal jährlich kostenlos Auskunft zu den bei ihnen ge-
speicherten Daten und Score-Werten geben.

Doch dies ist noch nicht ausreichend. Der Entwurf hat
drei entscheidende Schwachstellen, die sich in der Praxis
zum Nachteil des Einzelno aber auch der zuständigen
Datenschutzbeauftragten auswirken werden:

Es fehlt eine wirksame Beschränkung des Auskunftso-
marktes. Derzeit erlaubt das Gesetz eine Abfrage bei ei-
er Auskunftso, wenn das abfragende Unternehmen ein
berechtigtes Interesse geltend machen kann. Dieses wird
allzu oft in der Praxis im Sinne eines wirtschaftlichen Ri-
sikos ausgelegt. Dadurch wird das Risiko der Nicht-Leis-
tung einseitig auf die schwächere Vertragsparteien abge-
wälzt. So könnten in Zukunft auch Arbeitgeber vor einer
Einstellung die Bonität ihrer Arbeitnehmerinnen und Ar-
beitnehmer überprüfen. Die Schwierigkeit liegt in der
Praxis gerade darin, die aus allgemeinen wirtschaftlichen
Erwägung heraus begründeten Anfragen auf diejenigen
zu reduzieren, bei denen tatsächlich ein besonderes, weil
kreditorisches Risiko im Hintergrund steht. Hier fehlt
eine klare Beschränkung des Auskunftsomarktes. Des-
wegen sollte im Gesetz ein unmittelbares finanzielles
Ausfallrisiko wie Voraussetzung für eine Bonitätsauskunft
festgeschrieben werden.

Außerdem gehen die Auskunftsrechte an einer entschei-
denden Stelle noch nicht weit genug. Zwar soll der Score-
wert zukünftig einzelfallbezogen und nachvollziehbar er-
läutert werden, doch bei dieser sehr flexiblen und ausleg-
baren Bestimmung besteht die Gefahr, dass der Betrof-
fene nur mit einer allgemeinen Erklärung abgespeist
wird. Bereits heute erfährt der Betroffene bei einigen
Auskunftso auf Nachfrage, wie ein Score-Wert generell
zustande kommt. Für den Betroffenen kommt es aber dar-
auf an zu erfahren, welche Bedeutung eine bestimmte In-
führung für die Kreditentscheidung hat. Zum Schutz
Betriebs- und Geschäftsgeheimnisse wäre es genü-
gen, die genutzten Daten im absteigenden Reihen-
folge ihrer Bedeutung für das im Einzelfall berechnete
Ergebnis zu beaufsichtigen. Dies böte die Möglichkeit so-
wohl den Interessen der Wirtschaft nach einem Schutz
beim Score-Formel als auch den Transparenzanforderun-
gen der Bürgerinnen und Bürger gerecht zu werden.

Schließlich ist eine Beurteilung der Kreditwürdigung an-
hand der Wohnanschrift („Geo-Scoring“) diskriminierend
und unseriös, da sie die Bewertung der Kreditwürdigung
an ein Merkmal anknüpft, das der Einzeln nicht beein-
flussen kann (s. u. Nr. 7.1). Genau dies soll nach dem Ge-
setzentwurf aber möglich bleiben: Es ist gesellschaftlich
nicht hinnehmbar, dass man generell mehr für einen Kred-
it bezahlt, wenn man in einer schlecht beleumundeten
Gegend wohnt. Daher sollte die Verwendung von An-
schriften für die Bonitätsbewertung nicht zugelassen
werden.

Auch die Konferenz der Datenschutzbeauftragten des
Bundes und der Länder hat Nachbesserungen angemahnt.
Ich habe die Hoffnung, dass am Ende der zu Redaktions-
schluss noch andauernden Beratungen im Deutschen
Bundestag die Rechte der Betroffenen weiter gestärkt sein werden.

3.4.5 Informationelle Selbstbestimmung ernst nehmen – Neue Anforderungen an Werbewirtschaft und Adresshandel


3.4.6 Datenschutz bei Rechtsanwälten weiterhin nicht gesichert

Der Streit, ob auch Rechtsanwaltskanzleien dem Bundesdatenschutzgesetz und seinen Kontrollmechanismen unterliegen, konnte noch immer nicht gelöst werden.


Kasten zu Nr. 3.4.6

Aus der Stellungnahme der Bundesregierung zum 21. TB zu Nr. 9.7:

„Die Bundesregierung teilt die Rechtsauffassung des BfDI, dass die Erhebung und Verwendung personenbezogener – auch mandatsbezogener – Daten durch Rechtsanwälte den Vorschriften des BDSG unterliegen und dass die Datenschutzbehörden der Länder zuständig sind, die Datenschutzkontrolle durchzuführen. …“

Zwar hat sich die Bundesregierung in ihrer Stellungnahme zum 21. TB meiner Rechtsauffassung angeschlos
s (s. Kasten zu Nr. 3.4.6). Es ist aber noch nicht gelun-
gen, eine gesetzliche Klarstellung zu erreichen, so dass
das Grundrecht der betroffenen Bürgerinnen und Bürger
auf informative Selbstbestimmung bei Datenverarbeit-
tung durch Rechtsanwälte vielfach gar nicht oder nur sehr
geringfügig geltend gemacht werden kann. Dies gilt
nicht nur für die gesetzlichen Ansprüche auf Auskunft,
Benachrichtigung, Sperrung und Löschung von personen-
bezogenen Daten, sondern auch für die Möglichkeit, den
Umgang mit personenbezogenen Daten in Rechtsanwalts-
kanzleien durch die unabhängige Datenschutzaufsicht
überprüfen zu lassen.

Die Rechtsanwaltskammern vertreten die Meinung, dass
die Aufsicht in Bezug auf die mandatsbezogene Informa-
tionsverarbeitung bei Rechtsanwälten ausschließlich bei
ihnen liege. Unabhängig davon, ob weder das BDSG
noch die Europäische Datenschutzrichtlinie eine entspre-
chende Einschränkung der allgemeinen Regelungen ent-
halten, wäre ein solches Verfahren auch mit Artikel 28
Absatz 1 der Richtlinie unvereinbar, da die datenschutz-
rechtlichen Kontrollstellen ihre Aufgabe in völliger
Unabhängigkeit wahrnehmen müssen. Diese Unabhän-
gigkeit ist bei den Rechtsanwaltskammern als Selbstver-
waltungorganisation schon insoweit nicht gegeben, als
die Verantwortlichen von den Mitgliedern gewählt wer-
den, die zu Kontrollierenden also ihre Kontrolleure aus-
suchen und gegebenenfalls auch durch Abwahl sanktion-
nieren können.

Ein weiteres Argument der Rechtsanwaltskammern hat
großeres Gewicht: Es besteht die Sorge, die Aufsichtsbe-
hörden könnten verpflichtet sein, bei ihren Kontrollen ge-
wonnene Informationen, etwa über strafbare Handlungen
 eines Mandanten, an andere staatliche Stellen weiterzuge-
ben. Insofern bestehe auch kein Zeugnisverweigerungs-
recht und Beschlagnahmeverbot für die Aufsichtsbehör-
den. Auch wenn mir in der Praxis noch kein Fall bekannt
geworden ist, in dem sich dieses Problem konkret gestellt
hätte, kann dieses Argument rein rechtlich betrachtet
nicht völlig von der Hand gewiesen werden. Die Konse-
quenz kann allerdings nur sein, für die Datenschutzau-
sichtsbehörden entsprechende Schutzvorschriften zu
schaffen, durch die die Weitergabe entsprechender Er-
kenntnisse ausgeschlossen wird. Eine vergleichbare Pro-
blematisierung bestand auch hinsichtlich der Beschäftigung
externer Datenschutzbeauftragter durch Berufsgeheimnis-
träger. Hier hat der Gesetzgeber im Ersten Mittelstands-
S. 2970) u. a. in § 4f BDSG einen neuen Absatz 4a zum
Zeugnisverweigerungsrecht und Beschlagnahmeverbot
und in § 203 StGB einen neuen Absatz 2a zur Strafbarkeit
unbefugten Offenbarens durch Datenschutzbeauftragte
eingefügt. Ich hoffe, dass durch eine entsprechende Stär-
kung der Rechtstellung der Datenschutzaufsichtsbehör-
den auch hier eine für alle Seiten zufrieden stellende Lö-
sung gefunden werden kann.

Die in der Gegenübertragung der Bundesregierung zu mei-
nem 21. TB angekündigte Prüfung durch BMI und BMJ
hat offensichtlich auch nach zwei Jahren noch zu keinem
konkreten Ergebnis geführt. Dies bedauere ich um so
mehr, als der Streit für die Bürgerinnen und Bürger ganz
konkrete Konsequenzen hat. So habe ich bereits in mei-
nem letzten TB über den Fall einer Rechtsanwaltskanzlei
berichtet, die in großem Stil von der Deutschen Telekom AG für das Beitreiben ihrer Forderungen einge-
setzt wird und jede Zusammenarbeit mit der zuständigen
Datenschutzaufsichtsbehörde verweigert, obwohl es im-
mer wieder Besonderheiten wegen nicht ordnungsgemäßer
Datenverarbeitung gibt. Auch hier ist es trotz einer Viel-
zahl von Gesprächen, die u. a. von mir als zuständiger
Aufsichtsbehörde für die Deutsche Telekom AG mit die-
sen geführt wurden, noch zu keinem befriedigenden Er-
genommen. Nach meiner Überzeugung kann es im
Schutzbereich des BDSG und der Europäischen Daten-
enschutzrichtlinie keine datenschutz- und kontrollfreien
Räume geben. Es stellt sich deswegen die Frage, ob ein
Unternehmen wie die Deutsche Telekom AG im großen
Umfang personenbezogene Daten an einen Dritten über-
mitteln darf, wenn es nicht gewährleisten kann, dass die
Betroffenen dort den gleichen Datenschutz genießen, der
für das Unternehmen selber gilt.

3.4.7 Dringend notwendige Verbesserungen
beim Datenschutz in der Versicherungs-
wirtschaft lassen weiter auf sich warten

Die Verhandlungen zwischen Datenschutzaufsichtsbehör-
den und Versicherungswirtschaft über eine datenschutz-
gerechte Ausgestaltung der Datenverarbeitung bei den
Versicherungsunternehmen sind nun mühsam vorange-
kommen, befinden sich aber nun auf einem Erfolg ver-
 sprechenden Weg. Ein Durchbruch konnte indes noch
nicht erzielt werden.

Die Beratungen der AG Versicherungswirtschaft des
Düsseldorfer Kreises, einem Koordinierungsgremium der
Aufsichtsbehörden für den Datenschutz im nichtöffentli-
chen Bereich, mit dem Gesamtverband der Deutschen
Versicherungswirtschaft (GDV) wurden fortgesetzt. Ge-
genstand waren datenschutzrechtliche Fragen bei der Ver-
arbeitung personenbezogener Daten für Zwecke der
Antrags-, Vertrags- und Leistungsdarstellung durch die
Versicherungsunternehmen. Im Vordergrund standen der
Entwurf für eine neue einheitliche Einwilligungs-
und Schweigepflichtentbindungserklärung, die Umgestaltung
des früher unter dem Namen „Uniwagnis“ bekannten
Hinweis- und Informationssystems (HIS) und der Ent-
 wurf des GDV für Verhaltensregeln für den Umgang mit
personenbezogenen Daten im Sinne von § 38a BDSG

Über Struktur, Erscheinungsbild und Inhalt der Einwilli-
gungs- und Schweigepflichtentbindungserklärung sowie
des dazu gehörenden Merkblatts zur Datenverarbeitung
besteht zwischen der Versicherungswirtschaft und den
Datenschutzaufsichtsbehörden seit langem Dissens. Hier-
über habe ich bereits im 20. TB (Nr. 17.1.9) und 21. TB
(Nr. 9.6) berichtet. Die Datenschutzaufsichtsbehörden
fordern seit geraumer Zeit eine Änderung und Überarbei-
tung der Einwilligungserklärung, weil die bisher verwend-
dete Klausel nicht transparent genug ist und nicht den
Vorschriften des § 4a BDSG entspricht. Insbesondere un-
terscheiden sich die Auffassungen zu der Frage, welche
Datenverarbeitungen bereits nach den gesetzlichen Vor-
schriften zulässig sind und welche einer Einwilligung be-
dürfen. Ziel sollte es sein, die Einwilligungsklausel auf die
Sachverhalte zu beschränken, bei denen keine gesetz-
lichen Erlaubnistatbestände vorhanden sind (z. B. im Fall
der Nutzung und Übermittlung für Werbezwecke).

Die Entscheidung des Bundesverfassungsgerichts vom
23. Oktober 2006 zur Unzulässigkeit formularmäßiger
Einwilligungserklärungen in Verworrenungsverträgen
(1 BvR 2027/02, vgl. 21. TB Nr. 9.6) sowie das Inkraft-
treten von § 213 Versicherungsvertragsgesetz (VVG), in
der die Erhebung von Gesundheitsdaten durch Versiche-
rungsunternehmen geregelt wird, brachten endlich Beweg-
wung in die Diskussion und unterstützten die Daten-
schutzaufsichtsbehörden bei ihren Forderungen. Die im
Berichtszeitraum geführten Verhandlungen mit dem GDV
gestalteten sich dennoch schwierig und gingen nur müh-
sam voran. Grund hierfür waren die ebenfalls parallel dazu
laufenden Gespräche über die Verhaltensregeln der Versi-
cherungswirtschaft (s. u.) sowie die in unmittelbarem
Zusammenhang mit dem Umfang und Inhalt der Einwilli-
gungsklausel stehende Frage der Umgestaltung des Hin-
weis- und Informationssystems (HIS). Bei Redaktions-
schluss zeichnete sich jedoch ein erfolgreicher Abschluss
der Verhandlungen ab, so dass in Versicherungsverträgen
denächst die neue datenschutzgerechte Einwilligungs-
und Schweigepflichtentbindungserklärung nebst Merk-
blatt verwendet werden kann.

Über datenschutzrechtliche Bedenken gegen das Hein-
weis- und Informationssystem (HIS) der Versicherungswirt-
schaft, das der Risikoprüfung und Aufdeckung bzw.
Prävention von Versicherungsbetrag dient, habe ich im letzten
TB (Nr. 9.5) berichtet. Eine Bestandsaufnahme des Düsseldorfer Kreises hat diese Bedenken bestätigt
und die Datenschutzaufsichtsbehörden darin bestärkt,
eine datenschutzkonforme Umgestaltung des Systems zu
fordern. Nachdem der GDV Anfang 2007 erfreulicher-
weise seine Bereitschaft zu einer Neukonzeption erklärt
hatte, haben ihm die Datenschutzaufsichtsbehörden darin bestärkt,
dass die weitere Nutzung des bisherigen HIS für einen Übergangszeitraum bis Ende 2008 tolerieren
würden. Um zumindest vorläufig mehr Transparenz über
das bisherige Verfahren zu schaffen, haben der GDV und
und die AG Versicherungswirtschaft eine gemeinsame Ver-
fahrensbeschreibung erstellt und im Internet unter
www.gdv.de oder www.datenschutzzentrum.de veröffent-
licht.

Im November 2007 stellte der GDV seine Pläne zur
Neustrukturierung des Hinweis- und Informationssystems
vor, die als Grundkonzept eine Weiterführung als Aus-
kunftei nach § 29 BDSG vorsehen. Seitens der AG Versi-
cherungswirtschaft wurde signalisiert, dass dieses
Grundkonzept akzeptabel sei, jedoch noch zahlreiche De-
tailfragen geklärt werden müssten. Im September 2008
wies der GDV erstmals darauf hin, dass eine Inbetrieb-
nahme des neuen HIS Anfang 2009 unrealistisch sei. Im
November 2008, also knapp zwei Jahre nach dem Hin-
weis der Datenschutzaufsichtsbehörden auf die Rechts-
widrigkeit des bisherigen HIS, wurde schließlich mitge-
teilt, die Umsetzung des neuen Konzepts könne nicht vor
April 2011 abgeschlossen werden.

Es ist sehr zu bedauern, dass sich der GDV nun außer
Stände sieht, die von den Datenschutzaufsichtsbehörden
festgelegte Frist für die Aufnahme des dem Grunde nach
begrüßenswerten neuen HIS einzuhalten. Mit einer weite-
en Nutzung des bisherigen Systems wird ein daten-
schutzwidriger Zustand fortgeführt. Die Bereitschaft des
GDV zu datenschutzrechtlichen Verbesserungen in Bezug
auf die Benachrichtigung der Betroffenen bei Einmel-
dung in das System und auf eine Auskunftserteilung nach
§ 34 BDSG ändert nichts an der grundsätzlichen Rechts-
widrigkeit des derzeitigen Systems. Die AG Versiche-
rungwirtschaft hat den GDV im Dezember 2008 noch-
mals ausdrücklich auf den anhaltenden rechtswidrigen
Zustand hingewiesen, der sowohl die einzelnen Versiche-
rungsunternehmen als auch die zuständigen Aufsichts-
behörden im Falle der Weiternutzung des bisherigen HIS
vor große Probleme stellt. Wie die Aufsichtsbehörden im
einzelnen auf eine weitere Nutzung reagieren, war bei
Redaktionsschluss noch nicht absehbar. Einzelne Aufsichts-
behörden haben Versicherungsunternehmen aber
bereits darauf hingewiesen, dass sie einen fortgesetzten
rechtswidrigen Datenaustausch über HIS mit Sanktionen
belegen würden.

Positiv bewerte ich die Absicht des GDV, einen so ge-
nannten Code of Conduct für alle angeschlossenen Versi-
cerungsunternehmen zu erstellen. Hierbei handelt es
sich um Verhaltensregeln zur Förderung der Durchfüh-
rung datenschutzrechtlicher Regelungen im Sinne von
§ 38a BDSG. Eine solche Verhaltensrichtlinie schafft wei-
testgehend einheitliche Standards für die Verarbeitung
personenbezogener Daten beim Abschluss und bei der
Abwicklung von Versicherungsverträgen und fördert die
Einhaltung der zu beachtenden Datenschutzbestimmun-
gen. Sie wirkt zwar in erster Linie nach innen und richtet
sich an die Versicherungsunternehmen selbst. Sie ist aber
auch geeignet, dem Versicherungsnehmer einen Eindruck
to vertreiben, wie und auf welcher gesetzlichen Grund-
lage mit seinen persönlichen Daten verfahren wird. Die
Verhaltensregeln können zwar eine umfassende Unter-
richtung des Betroffenen nach § 4 Absatz 3 BDSG über
die Zweckbestimmung der Erhebung, Verarbeitung oder
Nutzung und die Kategorien von Empfängern nicht erset-
zten, bieten jedoch eine gute Möglichkeit, zusätzlich zur
neuen Einwilligungsklausel und zum Merkblatt die erfor-
derliche Transparenz der Datenverarbeitung zu erhöhen.

Der GDV hat der AG Versicherungswirtschaft Ende 2007
den Entwurf für den Code of Conduct zur Abstimmung
vorgestellt. Wegen des engen Zusammenhanges wurden
gemeinsame Gespräche hierüber zeitgleich mit den Berat-
tungen über den Inhalt der neuen Einwilligungs- und
Schweigepflichtentbindungserklärung geführt. Eine End-
fassung der Verhaltensregeln lag bei Redaktionsschluss
noch nicht vor.
Freiheit und Sicherheit

In den folgenden beiden Kapiteln berichte ich über Themen aus den Bereichen „Interner Sicherheit“ und „Recht und Verwaltung“. Schwerpunkte waren hier die Erweiterung der Befugnisse der Sicherheitsbehörden und insbesondere der heimliche Zugriff auf ein informationstechnisches System durch eine Sicherheitsbehörde (Nr. 4.1 ff.), die Neuregelung der Telekommunikationsüberwachung nach §§ 100a ff. StPO (Nr. 5.1), die geplante Einführung eines Zentralregisters im Bundesmeldegesetz (Nr. 5.2) und die Vorbereitungen für die Volkszählung im Jahr 2011 (Nr. 5.5).

4 Innere Sicherheit

4.1 Online-Durchsuchungen durch Sicherheitsbehörden

Online-Durchsuchungen sind schwerwiegende Grundrechtseingriffe und nur zur Abwehr existenzieller Bedrohungen zulässig.

Seit der Einführung der akustischen Wohnraumüberwachung 1998 (vgl. hierzu 20. TB Nr. 7.1) wurde keine einzelne Überwachungsmaßnahme so intensiv und kontrovers diskutiert wie der heimliche, d. h. vom Betroffenen unbemerkt, Zugriff auf ein informationstechnisches System (Personalcomputer, Mobiltelefon etc.) durch eine Sicherheitsbehörde, der sog. „Online-Durchsuchung“. Es handelt sich dabei regelmäßig um einen schwerwiegenden Grundrechtseingriff, wie das Bundesverfassungsgericht in seiner Entscheidung vom 27. Februar 2008 (1 BvR 370/07) festgestellt hat (s. o. Nr. 2.1). Der Begriff „Online-Durchsuchung“ umfasst nicht nur den einmaligen Zugriff auf ein System, um dort vorhandene Daten anzuschauen, zu kopieren oder auszuleiten. Er ermöglicht auch eine längerfristige Überwachung und damit die Erfassung aller während des Überwachungszeitraums erzeugten Daten (s. Kasten zu Nr. 4.1).

Kasten zu Nr. 4.1

Technische Voraussetzung für eine Online-Durchsuchung ist das Aufspielen einer entsprechenden Software in das zu überwachende System. Dies kann entweder über einen Datenträger (Diskette, CD-ROM, USB-Stick etc.) oder online, d. h. über eine bestehende Internet-Verbindung, z. B. als Anhang an eine E-Mail, geschehen. Der Betroffene merkt nichts hiervon. Er kann sich auch durch sog. Firewalls oder Virenschutzsoftware nicht hiergegen schützen.


Die für eine Online-Durchsuchung eingesetzte Software kann technisch bedingt auch höchsten persönlichen Daten erfasst, die zum Kernbereich der privaten Lebensgestaltung gehören. In diesen Kernbereich, der durch die in Artikel 1 des Grundgesetzes geschützte Menschenwürde garantiert wird, darf der Staat nicht eingreifen. Dies hat das BVerfG in mehreren Entscheidungen nachdrücklich betont.

Sollen mit der eingeschleusten Software ausschließlich Daten aus einem laufenden Kommunikationsvorgang (E-Mail-Verkehr, Internet-Telefonie) erfasst und ausgeleitet werden, spricht man von einer „Quellen-Telekommunikationsüberwachung“. Sie betrifft in erster Linie das durch Artikel 10 Grundgesetz geschützte Fernmeldegeheimnis. Ich halte es für zweifelhaft, ob technisch sichergestellt werden kann, dass bei einer Quellen-Telekommunikationsüberwachung ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird und es zu keiner Erhebung weiterer personenbezogener Daten, z. B. auf der Festplatte des betreffenden Rechners, kommt (s. u. Nr. 4.1.1; 8).


4.1.1 Verfassungsbeschwerde erfolgreich

Online-Durchsuchungsbefugnis im Landesverfassungsschutzgesetz Nordrhein-Westfalen ist verfassungswidrig.


Angesichts des schwerwiegenden Grundrechtseingriffs ist diese Maßnahme nur unter sehr engen Voraussetzungen zur Abwehr existenzieller Bedrohungen zulässig (s. o. Nr. 4.1). In meiner Stellungnahme gegenüber dem BVerfG habe ich nicht nur auf die gravierenden verwaltungsrechtlichen Mängel dieser gesetzlichen Befugnis, sondern auch auf meine generellen verfassungsrechtlichen Bedenken und die praktischen Probleme hingewiesen, die unvermeidbar mit der Durchführung von Online-Durchsuchungen verbunden sind. Ich begrüße es deshalb, dass das Gericht diese Bedenken aufgenommen und die Online-Durchsuchung nur in eng begrenzten Fällen und unter hohen Hürden für zulässig erklärt hat.
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten


7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht festgelegten Grenzen verfassungsrechtlich zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:
   - Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Artikel 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.
   - Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.
   - Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.
   - Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.
   - Für die Durchführung von „Quellen-Telekommunikationsüberwachungen“, die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.


4.1.2 Neue Befugnisse zur Online-Durchsuchung für das BKA

Die Diskussion über die dem BKA eingeräumte sog. Online-Durchsuchung zur Abwehr von Gefahren des internationalen Terrorismus (s. u. Nr. 4.3.1) kam erst nach Einschaltung des Vermittlungsausschusses zu einem (vorläufigen) Ergebnis. Jetzt wird sich wahrscheinlich das BVerfG damit befassen müssen.

An der Verfassungskonformität der Befugnisregelung zur Online-Durchsuchung in § 20k BKAG (Kasten zu Nr. 4.1.2) habe ich Zweifel. So verkürzt die hier vorgesehene Kernbereichsschutzregelung die verfassungsgeschichtlichen Vorgaben zum Schutz des Kernbereichs privater Lebensgestaltung in nicht akzeptabler Weise.


Zwar begrüße ich es, dass im Laufe des parlamentarischen Gesetzgebungsverfahrens Änderungen beschlossen wurden, wonach nunmehr die Anordnung der Online-Durchsuchung ausnahmslos dem Richtervorbehalt unterstellt wird und die Durchsicht der durch diese Maßnahme erlangten Daten auf kernbereichsrelevante Inhalte ebenfalls nur dem Richter obliegt. Der verfassungsrechtlich gebotene Schutz kernbereichsrelevanter Informationen auf der ersten Stufe schon bei der Datenerhebung bleibt jedoch weiterhin defizitär.


§ 20k BKA-Gesetz

Verdeckter Eingriff in informationstechnische Systeme

(1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen betrifft.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck noch erforderlich sind.

(4) Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(5) Die Maßnahme nach Absatz 1 darf nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden.

(6) Die Anordnung ergibt schriftlich. In ihr sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
4. die wesentlichen Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

4.1.3 Online-Durchsuchungen durch Nachrichtendienste

Die Vorgaben des Bundesverfassungsgerichts (s. o. Nr. 4.1) gelten auch für Nachrichtendienste. Online-Durchsuchungen ohne gesetzliche Grundlage sind rechtswidrig.


4.2.1 Bündelung der Telekommunikationsüberwachung beim Bundesverwaltungsamt

Das Vorhaben des BMI, Einrichtungen zur Telekommunikationsüberwachung durch Polizeien und Nachrichtendienste des Bundes und der Länder beim Bundesverwaltungsamt (BVA) zusammenzufassen, begegnet datenschutzrechtlichen Bedenken.


Daneben müssen noch weitere Fragen einer Lösung zugeführt werden.

Klärungsbedürftig ist u. a., in welchem Umfang das BVA im Rahmen seiner Beauftragung gegenüber dem jeweiligen Bedarfsträger weisungsgebunden ist. Ich halte es für problematisch, wenn nach dem Gesetzentwurf das BVA zwar den fachlichen und gesetzlichen Anforderungen des jeweiligen Auftraggebers Rechnung zu tragen hat, der einzelne Bedarfsträger jedoch keinen Anspruch darauf haben soll, dass das BVA seine technischen Einrichtungen nach dessen Wünschen konfiguriert. Im Hinblick auf die beim jeweiligen Bedarfsträger verbleibende Verantwortlichkeit bezüglich der Rechtmäßigkeit der Überwachungsmaßnahme sowie der dabei zu beachtenden Anforderungen an Datenschutz und Datensicherheit muss klar geregelt werden, dass das BVA den Weisungen des jeweiligen Bedarfsträgers zur Ausgestaltung der technischen Unterstützung, die dieser zur Wahrung seiner jeweiligen gesetzlichen Verpflichtungen für erforderlich hält, uneingeschränkt unterliegt. Entsprechende Vorkehrungen können, je nachdem auf welcher Rechtsgrundlage eine Telekommunikationsüberwachung durchgeführt wird, unterschiedlich hoch sein, so dass ein entsprechendes Auftragsverhältnis in jedem Einzelfall entsprechend ausgeostaltet sein muss. Der Bedarfsträger muss zudem die Möglichkeit haben, in einem laufenden Auftragsverhältnis ergänzende Maßnahmen vom BVA zu verlangen, etwa aufgrund geänderter Rechtsprechung, oder wegen neuer technologischer Entwicklungen.

Offen ist auch, in welchem Umfang die technischen Unterstützungsmassnahmen des BVA protokolliert werden und wie meine Beteiligungs- und Kontrollrechte bezüglich der Tätigkeit des BVA, etwa wenn das BVA Unterstützung bei Telekommunikationsüberwachungsmaßnahmen nach dem G 10-Gesetz oder für Landesbehörden leistet, gewährleistet werden.

Bei Redaktionsschluss waren die Ressortberatungen zu dem Gesetzentwurf noch nicht abgeschlossen.

4.2.2 Anti-Terror-Datei-Gesetz

Im Berichtszeitraum habe ich mich mit der Umsetzung des Ende 2006 in Kraft getretenen Anti-Terror-Datei-Gesetzes (ATDG) (vgl. 21. TB Nr. 5.1.1) befasst. Im Mittelpunkt stand dabei das Protokollierungsverfahren gemäß
§ 9 ATDG (Nr. 4.2.2.1). Schließlich habe ich auch im BKA eine Schwerpunktkontrolle der polizeilichen Datenverarbeitung in der Anti-Terror-Datei (ATD) durchgeführt (Nr. 4.2.2.2).

4.2.2.1 Die Protokollierung in der Anti-Terror-Datei gestaltet sich schwierig

Zwischen dem BMI und mir besteht ein Dissens hinsichtlich des Umfangs der nach § 9 ATDG erforderlichen Protokollierung sowie der Reichweite meiner datenschutzrechtlichen Kontrollbefugnis gemäß § 10 ATDG bezüglich dieser Protokolldaten.


Das BMI hat vorgeschlagen, dass die Landesdatenschutzbeauftragten die Protokolldaten, die durch Datenbanktransaktionen der jeweils ihrer Kontrollbefugnisse unterliegenden Landesstellen entstanden sind, im BKA selbst einsehen und auswerten können. Ich habe dieses Verfahren vorerst akzeptiert. Die nächsten Jahre werden zeigen, inwieweit dadurch eine effiziente Kontrolle der Datenverarbeitung in der ATD durch die daran beteiligten Bundes und Landesbehörden gewährleistet werden kann.

4.2.2.2 Kontrolle der Anti-Terror-Datei beim Bundeskriminalamt

Bei der Datenverarbeitung in der ATD habe ich einige datenschutzrechtliche Mängel festgestellt. Dies gilt insbesondere für die Problematik der Speicherung von „Randpersonen“.

Als ein zentraler Bestandteil der neuen Sicherheitsarchitektur des Bundes (vgl. 21. TB Nr. 5.1) wurde im März 2007 die Anti-Terror-Datei (vgl. 21. TB Nr. 5.1.1) durch den Bundesminister des Innern offiziell „freigeschaltet“. Zu Beginn wurden Informationen über rund 13 000 Personensätze in der ATD gespeichert; bis Ende Mai 2008 wuchs diese Zahl auf 17.745 an. Die Zahl der tatsächlich erfassten Betroffenen dürfte aber niedriger liegen, da einzelne Personen von verschiedenen Stellen
(mehrfach) gespeichert worden sein können. Dies ist be- dingt durch die Struktur der Datenbank.

Im März 2008 führte ich eine datenschutzrechtliche Kon- trolle der Datenverarbeitung in der ATD durch das BKA durch. Zu diesem Zeitpunkt hatte das BKA dort ca. 3 000 Datensätze eingegeben. Einen Schwerpunkt meiner Kontrolle bildete die Problematik der Speicherung von Kontaktpersonen und weiterer Randpersonen in der ATD, besonders unter dem Aspekt der Hinzuspeicherung von erweiterten Grunddaten. Hierbei wurden im Einzelnen die Kriterien „besuchte Orte oder Gebiete“, „Kontaktperso- 
n“ und „Bemerkungen/Hinweise“ sowie die Einstufung einer Person als „dolos“ Kontaktperson betrachtet.

„Besuchte Orte oder Gebiete“ nach § 3 Absatz 1 Num- mer 1 lit. b) nn) ATDG dürfen als erweiterte Grunddaten in der ATD gespeichert werden, sofern sich dort die in § 2 Satz 1 Nummern 1 und 2 ATDG genannten Personen treff- en. Ich habe bemängelt, dass in vielen der geprüften Fälle aus der Speicherung und den dazu vorgelegten Unterlagen nicht erkennbar war, ob die gespeicherten Ört- lichkeiten tatsächlich als Treffpunkte in diesem Sinne dienten.

Hingegen war die Speicherung von „Kontaktpersonen“ als erweitertes Grunddatum gemäß § 3 Absatz 1 Num- mer 1 lit. b) oo) ATDG in den geprüften Fällen nicht zu beanstanden. Die Voraussetzungen, dass zwischen der Kontaktperson und der Zielperson nicht nur flüchtige oder zufällige Verbindungen bestehen und dass es sich bei der Zielperson um eine „Hauptperson“ handelt, also um ein Mitglied einer terroristischen Vereinigung oder um ei- nen Befürworter von Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange, waren bei den geprüften Datensätzen für die Erfas- sung in der ATD erfüllt.

Bei den Speicherungen von „Bemerkungen/Hinweisen“ im Sinne von § 3 Absatz 1 Nummer 1 lit. b) rr) ATDG war nur in seltenen Fällen nachvollziehbar, warum dies – wie der Gesetzgeber voraussetzt – im Einzelfall nach pflichtgemäßem Ermessen von der Möglichkeit abhängt. Die Problematik bestand darin, dass bei der automatischen Befüllung der ATD mit einem Datensatz aus einer Quelldatei des polizeilichen Staatschutzes auch das dort gespeicherte Freitextfeld mit übertragen wurde, ohne dass die vom Gesetzgeber geforderte Einzelfallprüf- 

Das GASIM hat am 2. Mai 2006 in Berlin seine Arbeit aufgenommen. An ihm sind das Bundeskriminalamt, die Bundespolizei, das Bundesamt für Migration und Flücht- linge, die Finanzkontrolle Schwarzarbeit der Zollverwal- tung, der Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz und das Auswärtige Amt beteiligt. Das GASIM soll die Fachkompetenzen der beteiligten Behör-


Bis Redaktionsschluss hatte ich das umfangreiche Material, welches ich im Rahmen meines Beratungs- und Kontrollbesuchs eingesehen habe, noch nicht abschließend ausgewertet. Das Ergebnis der Kontrolle werde ich im nächsten Tätigkeitsbericht erörtern.

4.2.4 Neugestaltung der IT-Landschaft in der Abteilung Staatsschutz des Bundeskriminalamts

Das BKA richtet in der Abteilung Staatsschutz neue Dateien ein und nutzt hierfür das Programm rsCASE. Dadurch sollen Informationen besser verarbeitet und verteilt werden.


Auch in der Zukunft werde ich darauf achten, dass das BKA bei verbesserten technischen Datenverarbeitungsmöglichkeiten den durch das BKA-Gesetz gesteckten Rechtsrahmen einhält.

4.3 Bundeskriminalamt

Schanke ich der Tätigkeit im Berichtszeitraum waren die Novellierung des BKA-Gesetzes (s. u. Nr. 4.3.1) sowie die Fortentwicklung des polizeilichen Informationssystems INPOL (s. u. Nr. 4.3.2).
4.3.1 BKA-Gesetzesnovelle

Durch die Novellierung des BKA-Gesetzes werden dem BKA erstmals umfassende polizeiliche Befugnisse zur Abwehr des internationalen Terrorismus eingeräumt. Datenschutzrechtliche Kritik wurde dabei nur zum Teil berücksichtigt.

Die durch die Föderalismusreform vorgezeichnete Aufgabenverwaltung an das BKA bedeutet eine Zäsur in der bundesdeutschen Sicherheitsarchitektur (vgl. Kasten a zu Nr. 4.3.1). Die deutsche Polizei war in der Bundesrepublik Deutschland von Beginn an Ländersache. Die Zuweisung präventiver Befugnisse an das BKA verändert diese Kompetenzaufteilung, die letztlich auch öffentliche Gewalt begrenzende Ziele verfolgte.

Die BKA-Gesetzesbegehung begegnet vor allem zwei wesentlichen Kritikpunkten:

Ich habe weiterhin erhebliche Zweifel, inwieweit die vorgesehenen Datenerhebungs- und -verarbeitungsbefugnisse für die Erfüllung der vom BKA zugewiesenen Aufgaben wirklich angemessen, erforderlich und geeignet sind. Neben polizeilichen Standardbefugnissen, z. B. Platzverweis oder Personalienfeststellung, erhält das BKA zusätzlich besondere Ermittlungsbefugnisse bis hin zur Online-Durchsuchung informationstechnischer Systeme. Schon im Hinblick auf die weiterhin bestehende Zuständigkeit der Länder bei der Abwehr von Gefahren des internationalen Terrorismus ist fraglich, ob für die wenigen Fälle, in denen das BKA selbst tätig werden wird, diese Füße neuer Befugnisse wirklich angemessen ist.

So sind Eingriffsaufgaben mit großem zeitlichen Vorlauf, etwa die Rasterfähndung, nicht geeignet, um terroristische Bedrohungsanlagen schnell zu reagieren. Schutzpolizeiliche Standardbefugnisse setzen eine flächendeckende Präsenz des Amtes voraus, die faktisch nicht gegeben ist. Das Nebeneinander von Zuständigkeiten des BKA und der Landespolizeibehörden für die Gefahrenabwehr sehe ich auch insofern kritisch, als es dazu führt, dass sowohl das BKA als auch die Länder parallele Abwehrmaßnahmen ergreifen können und dabei gleich mehrfach personenbezogene Daten verarbeiten.


Schließlich geht es auch um das Verhältnis zwischen Prävention und Strafverfolgung. Bereits vor der Novelle hatte das BKA die Befugnis, in bestimmten Deliktsbereichen Ermittlungen vorzunehmen, allerdings unter der Verfahrensleitung der Generalbundesanwaltschaft und nach den Regeln der Strafprozessordnung. Zu diesen Deliktsbereichen zählt auch die Bildung terroristischer Vergehen. In diesen Fällen wäre das BKA also auf Gefahren abwehrende Befugnisse nicht angewiesen.

Kasten a zu Nr. 4.3.1

Ergebnis der Föderalismusreform


Artikel 73 GG wurde dazu wie folgt geändert:

cc) Nach Nummer 9 wird folgende Nummer 9a eingefügt:

„9a. die Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt in Fällen, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht;“. Der andere wesentliche Kritikpunkt an dem Gesetz betrifft die Gewährleistung des Kernbereichs privater Lebensgestaltung. Das Bundesverfassungsgericht hat in mehreren Entscheidungen in den letzten Jahren dem Gesetzgeber auferlegt, diesen Kernbereich bei heimlichen Datenerhebungs- und -verarbeitungsbefugnissen abzusichern, insbesondere indem Eingriffe in diesen Bereich soweit möglich von vorherin unterbleiben. Dieses Erhebungsverbot muss zudem durch Regelungen über die sofortige Löschung in- 

timer Informationen und der Nicht-Verwertbarkeit er- 

gänzt werden, wenn es ausnahmsweise doch zu einer Kernbereichsverletzung gekommen ist. Das BKA-Gesetz weist insofern Defizite auf. So verbleiben verfassungsrechtliche Zweifel daran, dass die Online-Durchsuchung informationstechnischer Systeme (s. o. Nr. 4.1.2) sowie der Überwachung der Telekommunikation nur unzulässig sein sollen, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass allein kernbereichsrelevante Inhalte erfasst werden. Da diese Fälle in der Praxis kaum vorkommen werden, läuft das Gebot, Eingriffe in den Kernbereich privater Lebensgestaltung grundsätzlich zu unterlassen, weitgehend ins Leere. Auch ist es aus meiner Sicht unzureichend, wenn im Zusammenhang mit der Er- 

hebung von Daten mit besonderen Mitteln gemäß § 20g BKG, wie z. B. längerfristige Observationen oder der Einsatz verdeckter Ermittler, von Regelungen zum Schutz des Kernbereichs völlig abgesehen wurde.

Diese Kritik wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geteilt (vgl. Kasten b zu Nr. 4.3.1).

Im Zuge des Gesetzgebungsverfahrens wurden aber auch – gemessen an den Vorentwürfen – einige Verbesserungen vorgenommen. So wurde die Gefahrenschwelle als Voraussetzung für die Durchführung einer Rasterfahn-
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Mehr Augenmaß bei der Novellierung des BKA-Gesetzes


Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehragegenstößen zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.


4.3.2 Polizeiliches Informationssystem INPOL

INPOL wird laufend fortentwickelt.


Daneben waren eine Reihe anderer Aspekte zu beachten, die sich auf den aktuellen Betrieb von INPOL beziehen. Dies betraf den erforderlichen Umfang der Protokollierung von Zugriffen (vgl. Nr. 4.3.2.1) sowie die Zulässigkeit der Speicherung personenbezogener Daten von Min derjährigen (vgl. Nr. 4.3.2.2).

4.3.2.1 Protokollierung im polizeilichen Informationssystem (INPOL)

Die Vorgabe der BKA-Gesetzesnovelle, dass jeder Zugriff auf das polizeiliche Informationssystem INPOL zu protokollieren ist, wirft die Frage auf, inwieweit auch die Inhalte von Datenfeldern protokolliert werden sollen.


Sowohl bei der fachlichen als auch bei der Nachrichtenprotokollierung werden auch die Inhalte der geänderten oder aufgerufenen Datenfelder erfasst. Hieran möchte das BKA auch festhalten, wenn künftig alle Zugriffe auf INPOL protokolliert werden.

Bei der Beurteilung der Erforderlichkeit einer Inhaltsprotokollierung der Datenbanktransaktionen sind die Möglichkeiten einer effektiven Datenschutzkontrolle sowie die Wahrung des Rechtsschutzinteresses der Betroffenen gegen die Entstehung paralleler Datenbestände und der damit einhergehenden Missbrauchsgefahren abzuwägen. Dabei ist nicht auszuschließen, dass ohne inhaltliche Protokollierung bei zwischenzeitlich gelöschten oder geän-

Da INPOL ein von Bund und Ländern gemeinsam betriebenes System ist, werde ich auf eine gemeinsame Position mit den Datenschutzbeauftragten der Länder hinwirken (Regelungen zur Protokollierung s. Kasten b zu Nr. 4.3.2.1).

### Kasten b zu Nr. 4.3.2.1

**Gesetzliche Regelungen zur Protokollierung von Datenabrufen aus Informationssystemen:**

- **Bundeskriminalamtsgesetz**
  
  § 11 Polizeiliches Informationssystem


- **Zollfahndungsdienstgesetz**
  
  § 11 Zollfahndungsinformationssystem


- **Bundesdatenschutzgesetz**

  *Anlage zu § 9 Satz 1 BDSG*

  Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, …

  5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle), …

  **§ 10 Einrichtung automatisierter Abrufverfahren**

  (2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

  1. Anlass und Zweck des Abrufverfahrens,
  2. Dritte, an die übermittelt wird,
  3. Art der zu übermittelnden Daten,
  4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

  Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.
4.3.2.2 Speicherung Strafunmündiger in INPOL

In einigen Verbunddateien des polizeilichen Informationsystems INPOL sollen künftig auch personenbezogene Daten von Strafunmündigen gespeichert werden. Dies begegnet datenschutzrechtlichen Bedenken.

In den Verbunddateien „Kriminalaktennachweis – KAN“ und „Analyse-System zur Verknüpfung von Gewaltverbrechen – VICLAS“ des polizeilichen Informationsystems INPOL sollen künftig auch personenbezogene Daten von Strafunmündigen, d.h. von Kindern unter 14 Jahren, als sog. sonstige Personen gemäß § 8 Absatz 5 BKA-Gesetz gespeichert werden (s. Kasten zu Nr. 4.3.2.2).

Das BKA hält die Speicherung Strafunmündiger dann für erforderlich, wenn von ihnen schwere Gewalttaten verübt werden und die dabei gezeigte kriminelle Energie die Annahme rechtfertigt, dass sie auch bei Eintritt der Strafmündigkeit Straftaten von erheblicher Bedeutung begehen werden.


Ich bedaure, dass das BMI meinen Bedenken nicht gefolgt ist. Nach Abschluss des Beteiligungsverfahrens mit den Ländern sind die geänderten Errichtungsanordnungen für die genannten Dateien vom BMI erlassen worden.

Kasten zu Nr. 4.3.2.2

§ 8 Absatz 5 BKA-Gesetz

(5) Personenbezogene Daten sonstiger Personen kann das Bundeskriminalamt in Dateien speichern, verändern und nutzen, soweit dies erforderlich ist, weil bestimmte Tatsachen die Annahme rechtfertigen, dass die betreffen den Straftaten von erheblicher Bedeutung begehen werden.

4.3.2.3 Noch immer keine Rechtsverordnung gemäß § 7 Absatz 6 BKAG

Mit der Rechtsverordnung gemäß § 7 Absatz 6 BKAG hat das BMI das Nähere über die Art der Daten, die in INPOL gespeichert werden dürfen, festzulegen.


Im Rahmen der Anhörungsverfahren zu Errichtungsanordnungen für Verbunddateien des polizeilichen Informationssystems INPOL habe ich immer wieder das Fehlen der entsprechenden Rechtsverordnung moniert. Die Auf fassung des BMI, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, sondern im Hinblick auf die übrigen Regelungen des BKA-Gesetzes nur deklatorische Bedeutung habe, wird weder durch den Wortlaut der einschlägigen Regelungen noch durch die Gesetzesmaterialien zum BKA-Gesetz gestützt.

Eine nähere Bestimmung der Art der Daten, die in Verbunddateien verarbeitet werden dürfen, erfolgt durch das


Bereits vor der Gesetzesänderung hatte ich stets für ein differenziertes Vorgehen plädiert, orientiert insbesondere am Gefährdungsgrad der überwachten Örtlichkeiten. Leider wurde diese Anregung bei der in aller Eile, ohne angemessene parlamentarische Beratung, beschlossenen Gesetzesänderung nicht aufgegriffen.

Allerdings begrüße ich es, dass die Bundespolizei meine Anregungen insoweit aufgegriffen hat, als nach den Mus tererrichtungsanordnungen für die dateimäßige Verarbeitung von Daten aus der Videoverwachung von Bahnanlagen oder Flughäfen grundsätzlich eine nur zehntägige Speicherdauer festgelegt hat, die nur bei besonderen Anlässen auf 30 Tage ausgedehnt werden darf.

Der Einsatz von Videokameras durch die Bundespolizei soll auch auf Flughäfen erweitert werden. Dabei soll die Bundespolizei – ähnlich wie bei Anlagen der Deutschen Bahn AG (vgl. 21. TB Nr. 4.2 f.) – auf die Überwachungskameras der privaten Betreiber des Dritte Gesetzes zur Änderung des Bundespolizeigesetzes zurückgreifen, wofür eine besondere Nutzungsvereinbarung nötig ist.

Ich begrüße auch die Zuschirmung des BMI, dass neu zu beschaffende Videokameras die Anforderungen des von mir entwickelten datenschutzrechtlichen Profils „Common Criteria Protection Profile Software zur Verarbeitung von personenbezogenen Bild- und Audio-Daten“ erfüllen sollen (s. auch Nr. 8.1).

4.4 Bundespolizei – Noch mehr Videoüberwachung

Nach einer Änderung des Bundespolizeigesetzes darf die Bundespolizei Daten aus Videoüberwachungsanlagen bis zu einem Monat speichern. Auch auf Flughäfen soll der Einsatz von Videotechnik zu Überwachungszwecken ausgeweitet werden.


Bereits vor der Gesetzesänderung hatte ich stets für ein differenziertes Vorgehen plädiert, orientiert insbesondere am Gefährdungsgrad der überwachten Örtlichkeiten. Leider wurde diese Anregung bei der in aller Eile, ohne angemessene parlamentarische Beratung, beschlossenen Gesetzesänderung nicht aufgegriffen.

Allerdings begrüße ich es, dass die Bundespolizei meine Anregungen insoweit aufgegriffen hat, als nach den Mustererrichtungsanordnungen für die dateimäßige Verarbeitung von Daten aus der Videoverwachung von Bahnanlagen oder Flughäfen grundsätzlich eine nur zehntägige Speicherdauer festgelegt hat, die nur bei besonderen Anlässen auf 30 Tage ausgedehnt werden darf.

Der Einsatz von Videokameras durch die Bundespolizei soll auch auf Flughäfen erweitert werden. Dabei soll die Bundespolizei – ähnlich wie bei Anlagen der Deutschen Bahn AG (vgl. 21. TB Nr. 4.2 f.) – auf die Überwachungskameras der privaten Betreibergesellschaft zurückgreifen, wofür eine besondere Nutzungsvereinbarung nötig ist.

Ich begrüße auch die Zuschirmung des BMI, dass neu zu beschaffende Videokameras die Anforderungen des von mir entwickelten datenschutzrechtlichen Profils „Common Criteria Protection Profile Software zur Verarbeitung von personenbezogenen Bild- und Audio-Daten“ erfüllen sollen (s. auch Nr. 8.1).

4.5 Ermittlungsverfahren der Generalbundesanwaltschaft

Bei Ermittlungsverfahren der Generalbundesanwaltschaft stellt sich die Frage der Rechtmäßigkeit des Vollzugs von Postbeschlagnahmen sowie der Durchführung der Telekommunikationsüberwachung.


Nach Prüfung der Sach- und Rechtslage habe ich in der Angelegenheit keinen datenschutzrechtlichen Verstoß festgestellt und mich der Auffassung der Generalbundesanwaltschaft angeschlossen, dass diese Maßnahme in Einklang mit den §§ 99, 100 StPO stand. Die Beschlagnahmenordnung betraf ausschließlich solche Postsen-
dungen, die nach ihrem äußeren Erscheinungsbild durch das Fehlen eines Absenders gekennzeichnet waren. Dieses Aussonderungskriterium schloss aus, dass bei der Inaugenscheinnahme durch Polizeibeamte der briefliche Kommunikationsvorgang zwischen identifizierbaren Personen bewusst zur Kenntnis genommen wurde. Das kurzzeitige Betrachten eines Briefumschlags zur Feststellung des Vorhandenseins einer Absenderangabe stellt keine staatliche Kenntnismahme oder Erfassung eines Kommunikationsvorganges und damit keinen Eingriff in das durch Artikel 10 GG geschützte Brief- und Postgeheimnis dar. Auch die Art und Weise der Öffnung des beschlagnahmten Briefes entsprach dem Regelungsgehalt des § 100 Absatz 3 StPO.


Die Generalbundesanwaltschaft vertrat hierzu die Auffassung, dass die richterliche Durchführung richterlicher Ermittlungsanordnungen und der Staatsanwaltschaft schließlich die Verbindungsdaten und Gesprächsinhalte sämtlicher mit einem Beweiswertungsverbot belegten Verbindungen gelöscht. Auf meinen Hinweis hin wurden im BKA auf Anordnung der Staatsanwaltschaft schließlich die Verbindungsdaten und Gesprächsinhalte sämtlicher mit einem Beweiswertungsverbot belegten Verbindungen gelöscht.

4.6 Bundeszentralregister beim Bundesamt für Justiz

Durch Novellierung des Bundeszentralregistergesetzes (BZRG) soll die Erteilung eines „erweiterten Führungszeugnisses“ für Personen ermöglicht werden, die aufgrund beruflicher oder ehrenamtlicher Tätigkeit in einem besonderen Näheverhältnis zu Kindern und Jugendlichen stehen.


4.7 Nachrichtendienste

4.7.1 Bundesamt für Verfassungsschutz

Bei der Erteilung von Auskünften an die Betroffenen legt das Bundesamt für Verfassungsschutz (BfV) einen zu strengen Maßstab an und missachtet damit einen bereits im Jahre 1993 gefassten Beschluss des Deutschen Bundestages.


Ich habe daher das BfV aufgefordert, seine Auskunftspraxis verfassungsconform auszustellen. Eine Antwort hierzu lag bei Redaktionsschluss nicht vor.

4.7.2 Militärischer Abschirmdienst

Im Rahmen meiner Anhörung zu einer Dateianordnung hat das BMVg sich geweigert, mir eine zwischen dem MAD und dem BND getroffene Vereinbarung über die Zusammenarbeit bei besonderen Auslandsverwendungen der Bundeswehr zu überlassen. Dies habe ich als schwerwiegenden Verstoß gegen die in § 24 Absatz 4 BDSG normierte Mitwirkungspflicht förmielo beanstandet. Eine andere Regelung in dieser Dateianordnung ist mit dem Grundrecht auf informationelle Selbstbestimmung nicht vereinbar.

Nach § 8 MADG hat der MAD für jede automatisierte Datenarchivierung personenbezogene Daten eine Dateianordnung nach § 14 BVerfSchG zu erstellen, der die Zustimmung des BMVg bedarf und vor deren Erlass ich anzuholen bin. So hat mir das BMVg den Entwurf einer Anordnung für eine Datei zur Anhörung zugeleitet, die als Auswerte- und Organisationsmittel zur Aufgabenerfüllung des MAD während einer besonderen Auslandsverwendung der Bundeswehr gemäß § 14 Absatz 1 MADG genutzt wird. Bei der Anordnung der Bundeswehr arbeiten MAD und BND eng zusammen. Die Einzelheiten dieser Zusammenarbeit sind für jeden Einsatz in einer Vereinbarung mit dem MAD und dem BND zu regeln, die der Zustimmung des Chefs des Bundeskanzleramtes und des BMVg bedarf und über die das Parlamentarische Kontrollgremium zu unterrichten ist (§ 14 Absatz 6 Satz 4 MADG).

Im Rahmen des Anhörungsverfahrens habe ich das BMVg um Übersendung der für diesen Auslandsein satz geschlossenen Vereinbarung gebeten. Dies hat das BMVg mit der Begründung abgelehnt, ein Zusammenhang mit meiner „informatorischen Beteiligung“ am ministeriellen Gegenstandsverfahren der Dateianordnung und der für die Auslandseinsätze der Bundeswehr mit dem BND abgeschlossenen Vereinbarung sei nicht erkennbar. Im Übrigen enthalte die Vereinbarung keine Regelung zum Umgang mit personenbezogenen Daten.

Kasten zu Nr. 4.7.2

§ 6 Absatz 2 MADG

(2) In Dateien oder zu ihrer Person geführten Akten gespeicherte Daten über Minderjährige sind nach zwei Jahren auf die Erforderlichkeit der Speicherung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, dass nach Eintritt der Volljährigkeit weitere Erkenntnisse nach § 1 Absatz 1 oder § 2 angefallen sind. Dies gilt nicht, wenn der Betroffene nach § 1 Absatz 3 überprüft wird. Die Speicherung personenbezogener Daten über Minderjährige vor Vollendung des 16. Lebensjahres in zu ihrer Person geführten Akten und Dateien ist unzulässig.
Abgesehen davon, dass es sich bei meiner Anhörung nicht um eine informatorische Beteiligung, sondern um eine nach § 8 MADG, v. F. § 14 Absatz 1 Satz 2 BVerfSchG institutionalisierte formale Anhörung handelt, verstößt die Weigerung des BMVg gegen § 24 Absatz 4 BDSG. Nach dieser Vorschrift haben die öffentlichen Stellen des Bundes mich bei meiner Aufgaben-erfüllung zu unterstützen und mir dabei Auskunft zu meinen Fragen sowie Einsicht in alle Unterlagen zu gewähren. Zu diesen Unterlagen gehört auch die hier in Rede stehende Vereinbarung zwischen dem MAD und dem BND. Da mir das BMVg auch nach wiederholter Bitte die Vereinbarung nicht zugänglich gemacht hat, habe ich dies als schwierigstes Verstoß gegen die Mitwirkungspflicht gemäß § 25 Absatz 1 BDSG förmlich beanstandet.

In seiner Erwiderung vertritt das BMVg die Auffassung, ein Verstoß gegen die Mitwirkungspflicht liege nicht vor. Gleichwohl hat es mir ohne Anerkennung einer rechtlichen Verpflichtung eine Mustervereinbarung nach § 14 Absatz 6 MADG zur Zusammenarbeit von MAD und BND bei besonderen Auslandsverwendungen der Bundeswehr übersandt. Dies ist jedoch nicht ausreichend, da die datenschutzrechtlichen Regelungen von mir nur in Bezug auf die konkreten im Auslandeinsatz getroffenen Vereinbarungen betrachten können. Im Übrigen hat sich gezeigt, dass bereits die übersandte Mustervereinbarung entgegen der Beklarungen des BMVg Rege- lungen zum Umgang mit personenbezogenen Daten enthält bzw. darauf ausgerichtet ist. Das BMVg beharrt dennoch auf seiner Weigerung.

Bei einem anderen Punkt dieser Dateianordnung habe ich mit Blick auf das MADG verfassungsrechtliche Zweifel. Die Dateianordnung sieht vor, dass eine Berichtigung, Löschung oder Sperrung der in der Datei gespeicherten Daten innerhalb einer deutschen Staatsangehörigkeit, ohne Rücksicht auf die Auslandslage, vorgenommen werden kann. Ich habe mich dieser Annahme aus mehreren Gründen skeptisch geäußert. Erstens, die Annahme, dass sich Personen in Auslandliege bis zu ihrer deutschen Staatsangehörigkeit verhalten, ist in der kollektiven Fähigkeit der Bundeswehr nicht realisierbar. Zweitens, die Annahme, dass sich die Vereinbarung auf die deutsche Staatsangehörigkeit bezieht, ist nicht durch die Dateianordnung nachvollziehbar. Drittens, die Annahme, dass sich die Vereinbarung auf die deutsche Staatsangehörigkeit bezieht, ist nicht durch die Dateianordnung nachvollziehbar.

4.7.3 Bundesnachrichtendienst

4.7.3.1 Überwachung von Journalisten

Eine über mehrere Jahre andauernde Überwachung eines Journalisten durch den BND war rechtswidrig.


4.7.3.2 Auskunftsverpflichtung des BND auch bezüglich Akten


Im Lichte dieser Entscheidung sollte § 7 BNDG bei der demnächst zu erwartenden Novellierung eindeutig geändert werden.

4.8 Sicherheitsüberprüfung

4.8.1 Notwendigkeit zur Änderung des SÜG

Mit dem Ausscheiden eines Betroffenen aus einer sicherheitsempfindlichen Tätigkeit muss die Nachberichtspflicht enden. § 18 Absatz 5 SÜG, wonach die mitwirkende Behörde erst fünf Jahre nach dem Ausscheiden aus der sicherheitsempfindlichen Tätigkeit zu unterrichten ist, verhindert dies jedoch.


Ich bedauere es, dass das BMI meine Anregung nicht aufgegriffen hat. Die Nachberichtspflicht sei zwingend erforderlich, um im Verjährungszeitraum bei der mitwirkenden Behörde nachträglich anfallende sicherheitsrelevante Erkenntnisse durch die zuständige Stelle daraufhin prüfen zu können, ob auf Grund dieser Erkenntnisse ein Geheimnissverrat begangen worden sein könnte und daher strafrechtliche Ermittlungen veranlasst werden müssten. Der Grund für die fünfjährige Frist liegt in der Verjährungsfrist für den Tatbestand des Geheimnissverrats nach § 353b StGB.


Ich werde daher weiterhin auf eine Änderung des § 18 Absatz 5 SÜG drängen.

4.8.2 Kontrollen

Bei meinen Kontrollen von Sicherheitsüberprüfungen gemäß § 18 SÜG habe ich wie bereits in der Vergangenheit Fehler festgestellt.

Im Berichtszeitraum habe ich Kontrollen der Sicherheitsüberprüfungsverfahren im öffentlichen und im nicht-öffentlichen Bereich durchgeführt. Dabei habe ich erstmals auch Sicherheitsüberprüfungen im Rahmen des durch das Terrorismusbekämpfungsaktetat 2002 eingeführten vorbeugenden personellen Sabotageschutzes nach § 1 Absatz 4 SÜG kontrolliert (vgl. 19. TB Nr. 20.1).


So habe ich mehrfach festgestellt, dass Lösungs- bzw. Vernichtungsfristen nicht eingehalten wurden, weil der Geheimschutzbeauftragte oder der Sicherheitsbevollmächtigte das Ausscheiden eines Mitarbeiters aus der si-
cherheitsempfindlichen Tätigkeit nicht rechtzeitig erfah-
ren hatte oder das tatsächliche Datum des Ausscheidens
nicht eindeutig festgestellt worden war (vgl. 21. TB
Nr. 5.8.3.2). Ich begrüße es, dass das BMI nunmehr alle
obersten Bundesbehörden darauf hingewiesen hat, dass
beim Ausscheiden von Mitarbeitern aus der sicherheits-
empfindlichen Tätigkeit der Geheimschutzbeauftragte
unverzüglich zu informieren ist.

Ein weiteres Problem hat sich erneut beim Zugriff des
Geheimschutzbeauftragten auf das jeweilige elektronici-
sche Personalverwaltungssystem gezeigt (vgl. 21. TB
Nr. 5.8.3.2). Bei dem von mir kontrollierten Bundespoli-
zieipräsidium hatte der Geheimschutzbeauftragte Zugriff
auch auf bestimmte Daten zu Personen, die nicht der Ge-
heimschutzbetreuung unterlagen. Nach meiner Interven-
tion wurde der lesende Zugriff des Geheimschutzbeauf-
tragten auf das System wieder unterbunden.

Da ich befürchte, dass eine derartige Praxis auch bei an-
deren Behörden und Unternehmen besteht, bedarf es ei-
er eindeutiger genereller Regelung, ob und in welchem
Umfang dem Geheimschutzbeauftragten bzw. dem Si-
cherheitsbevollmächtigten Zugriff auf das Personalver-
waltungssystem zu gestatten ist.

Bei meiner Kontrolle eines Bundespolizeipräsidiums im
Jahre 2005 hatte ich bemängelt, dass dort Personalmitte-
lungen, Veränderungsanzeigen und dergleichen durch die
Personalverwaltung sowohl dem Geheimdienstverwaltungs-
amt als auch anderen Stellen (z. B. Personalrat, Ver-
trauensperson der Schwerbehinderten) oft in Form von
Sammelverfügungen zur Kenntnis gebracht wurden
(vgl. 21. TB Nr. 5.8.3.1). Leider musste ich bei der Kon-
trolle eines anderen Präsidiums im Jahr 2007 den glei-
chen Mangel feststellen. Von einer Beanstandung nach
§ 25 BDSG habe ich abgesehen, nachdem das BMI alle
Dienststellen der Bundespolizei verpflichtet hatte, den
Geheimschutzbeauftragten ausnahmslos nur solche Infor-
mationen zugänglich zu machen, die im Einzelfall eine si-
cherheitsüberprüfte Person betreffen und die für Belange
des Geheimdienstes relevant sind. Des Weiteren hat das
BMI die Dienststellen verpflichtet, bei Sammelverfüge-
ungen die Namen Dritter vor Weitergabe an den Geheim-
dienstbeauftragten unkenntlich zu machen.

Bei zwei von mir kontrollierten Unternehmen teilsich die
Sicherheitsbevollmächtigten das Büro – wenn auch
zum Teil nur zeitweilig – mit anderen Mitarbeitern, die
nieht auf Aufgaben der Sicherheitsüberprüfung bestraft
sind. Dies halte ich im Hinblick auf die strengen Aufla-
gen zur Aufbewahrung von Sicherheitsunterlagen (§ 30
i. V. m. § 19 Absatz 1 SÜG) für bedenklich. Bei der Mit-
betreuung des Büros des Sicherheitsbevollmächtigten
durch eine weitere Person ist – auch bei aller Sorgfält-
lich nicht auszuschließen, dass diese Person Einblick in die
Sicherheitsakten und den vom Sicherheitsbevollmächtig-
ten benutzten PC nehmen kann. Zudem kann diese
Person durch das Mitführen von im Einzelfall unvermeidbaren
Telefonaten und Gesprächen Kenntnis von vertraulichen

Inhalten erlangen. Ich habe daher das BMWi gebeten, bei
den kontrollierten Unternehmen für entsprechende orga-
nisatorische Änderungen zu sorgen.

Ein grundsätzliches Problem hat sich bei der Kontrolle
eines Unternehmens gezeigt, das selbst keine
Verschlusssachen (VS) verwaltet. Dennoch waren alle
Geschäftsführer einer Sicherheitsüberprüfung unterzo-
gen worden. Das BMWi rechtfertigt dies damit, dass die
Überprüfung der Geschäftsleitung nach Nr. 4.1.3
Absatz 1 des Geheimdiensthandbuchs als Teil der Zu-
verlässigkeitüberprüfung eines Unternehmens aus-
rücklich vorgesehen sei. Da die Konsistenz der Überprü-
fung der Geschäftsleitung nach der höchsten VS-Einstufung der VS-Aufräge des Unter-
nehmens. Bei der kontrollierten Unternehmen keine VS ver-
waltet, halte ich es für fragwürdig, wenn Geschäftsfüh-
er von Unternehmen ohne materiellen Geheimdienst
einer Sicherheitsüberprüfung unterzogen werden. Da sie
keinen Zugang zu VS haben und auch der vorbeugende
personelle Sabotageschutz ausscheidet, sehe ich hierzu
keine Notwendigkeit. Auch der – höchst theoretische –
Fall, dass ein Mitglied der Geschäftsleitung im Einzel-
fall Zugang zu einem betreuten Unternehmen mit mate-
rilem Geheimdienst bekommt, rechtfertigt nicht die
Durchführungen einer Sicherheitsüberprüfung, die mit
erheblichen Eingriffen in das Persönlichkeitsrecht verbun-
den ist. Sollte die Sicherheitsüberprüfung der Ge-
schäftsführer mehr den Charakter einer Zeugniss-
überprüfung haben, sah ich hierfür keine gesetzliche Grundlage (vgl. hierzu Nr. 4.8.3.2).

Ich habe das BMWi zu einer weiteren Stellungnahme auf-
gefordert, die aber bei Redaktionsschluss noch nicht vor-
lag.

4.8.3 Sicherheitsüberprüfungen außerhalb
des SÜG

Bei Sicherheits- bzw. Zuverlässigkeitsüberprüfungen gibt
es einen zunehmenden Wildwuchs. Teilweise stehen Zu-
verlässigkeitsüberprüfungen aber auch mit dem gelten-
den Recht nicht in Einklang.

Zahlreiche Gesetze und Verordnungen enthalten Regelun-
gen zur Überprüfung der Zuverlässigkeit von Personen. Die
wichtigsten Regelungen mit detaillierten Verfahrens-
vschriften sind das Sicherheitsüberprüfungsgesetz, das
Luftfahrtübersichtsgesetz (LuftSÜG) und das Atomgesetz (AtG).
Obwohl die Zielsetzung dieser Vorschriften in weiten
Teilen übereinstimmen, weichen die materiellrechtlichen
Regelungen und die Verfahrensvorschriften zum Teil er-
heblich voneinander ab. Nachdem im Jahre 2002 durch
das Terrorismusbekämpfungsgesetz der vorbeugende per-
sonelle Sabotageschutz in das SÜG aufgenommen wurde
(vgl. 19. TB Nr. 20.1), stellt sich die Frage, ob weiterhin
Vorhaben entsprechende Regelungen zur Zuverlässigkeitsüberprü-
fung von Personen außerhalb des SÜG sinnvoll und erfor-
derlich sind, da es sich bei den Überprüfungen nach dem

Drucksache 16/12600 – 64 – Deutscher Bundestag – 16. Wahlperiode
LuftSiG und dem AtG um Varianten des vorbeugenden personellen Sabotageschutzes handelt.


4.8.3.1 Atomgesetz

Die vorgesehenen Gesetzesänderungen für atomrechtliche Zuverlässigkeitsüberprüfungen sind datenschutzrechtlich unbefriedigend.


- Die zuständigen Behörden dürfen die zur Überprüfung erhobenen personenbezogenen Daten speichern und nutzen, soweit dies für die Überprüfung erforderlich ist. Im Gegensatz zu den Regelungen im SÜG, in denen im Einzelnen enumerativ aufgeführt ist, wer welche Daten speichern darf (vgl. § 20 SÜG), wird hier die Befugnis zur Speicherung von personenbezogenen Daten erheblich ausgeweitet. Auch dies steht im Widerspruch zum vorgenannten Volkszählungsurteil, wonach es mit dem informationellen Selbstbestimmungsrecht nicht vereinbar ist, wenn der Bürger nicht mehr wissen kann, wer, was, wann und bei welcher Gelegenheit über ihn weiß. Insbesondere habe ich Bedenken, wenn die von angefragten Stellen mitgeteilten Erkenntnisse, die vielfach äußerst sensibel sind und zum Teil auch aus dem nachrichtendienstlichen Vorfeld stammen, automatisiert und damit voll recherchierbar gespeichert werden. Der Gesetzgeber hat beim SÜG die Gefahren, die von einer automatisierten Informationsverarbeitung für das informationelle Selbstbestimmungsrecht ausgehen, gesehen und deshalb die automatisierte Speicherung von personenbezogenen Daten durch die zuständige Stelle auf die Personengrunddaten beschränkt. Entsprechendes sollte auch hier vorgesehen werden.

4.8.3.2 Zuverlässigkeitsüberprüfungen ohne gesetzliche Grundlage

Einwilligungen der Betroffenen können Zuverlässigkeitsüberprüfungen bei Großveranstaltungen oder durch Arbeitgeber nicht legitimieren. In einem Fall habe ich eine fälschliche Beanstandung ausgesprochen.

Im 21. TB (Nr. 5.2.5) hatte ich über die Zuverlässigkeitsüberprüfungen anlässlich der Fußball-Weltmeisterschaft 2006 berichtet und Zweifel geäußert, ob die Einwilligung der zu akkreditierenden Personen eine ausreichende Rechtsgrundlage für diese Überprüfungen – insbesondere im Hinblick auf die Beteiligung des Verfassungsschutzes und des BND – darstellte. Wegen der Einmaligkeit dieses Ereignisses hatte ich diese Eingriffsmafnahmen aber noch als hinnehmbar angesehen, zumal die Betroffenen umfassend informiert worden waren.

Kasten a zu Nr. 4.8.3.2


Zuverlässigkeitsüberprüfungen bei Großveranstaltungen


Ich habe die Deutsche Bundesbank daher aufgefordert, das Verfahren zur Zuverlässigkeitsüberprüfung unverzüglich einzustellen und die insoweit rechtswidrig erhobenen personenbezogenen Daten der Betroffenen zu löschen und zu vernichten. Die Deutsche Bundesbank ist in Übereinstimmung mit dem BMI der Auffassung, dass die Zuverlässigkeitsüberprüfungen in rechtmäßiger Weise erfolgen und die Schaffung einer besonderen Rechtsgrundlage nicht erforderlich sei. Da die Deutsche Bundesbank an dem Verfahren weiter festhält, habe ich dies nach § 25 BDSG förmlich beanstandet.

Kasten b zu Nr. 4.8.3.2


Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern


5 Rechtswesen und Innere Verwaltung

5.1 Telekommunikationsüberwachung und andere heimliche Ermittlungsmaßnahmen nach der StPO


Im Februar 2008, also erst nach Abschluss des Gesetzgebungsverfahrens zur Neuregelung der heimlichen Ermittlungsmaßnahmen, hat das BMJ eine Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg zur „Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO“ veröffentlicht (Bundestagsdrucksache 16/8434). Das Gutachten bestätigt die datenschutzrechtliche Kritik an der Ausgestaltung der Verkehrsdatenaufgabe zu Strafverfolgungszwecken. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die maßgeblichen Ergebnisse der Studie und die hieraus von Gesetzgeber und Praxis zu ziehenden Konsequenzen in einer Entschließung vom 6./7. November 2008 in Einzelnen dargestellt (vgl. Kasten b zu Nr. 5.1). Ich appelliere an die Bundesregierung, die Regelung des § 100g StPO unter diesen Aspekten zügig nachzubessern.

Vorratsdatenspeicherung, Zwangidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen


Zwar stärken einige der vorgesehenen Änderungen der Strafprozessordnung die rechtstaatlichen und grundrechtlichen Sicherungen bei verdeckten strafprozessualen Ermittlungsmaßnahmen. Es besteht jedoch noch erheblicher Verbesserungsbedarf, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, den Schutz von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern und die Voraussetzungen der Telekommunikationsüberwachung:

– Mit einer erneuten Ausweitung des Straftatenkatalogs für die Telekommunikationsüberwachung würde die Tendenz zunehmender Überwachungsmaßnahmen in verstärktem Maße fortgesetzt. Der Katalog sollte deshalb mit dem Ziel einer deutlichen Reduzierung kritisch überprüft werden. Es sollten nur Straftaten auf genommen werden, deren Aufklärung in besonderem Maße auf die Telekommunikationsüberwachung angewiesen ist, die mit einer bestimmten gesetzlichen Mindeststrafe (z. B. ein Jahr) bedroht sind und die auch im Einzelfall schwer wiegen.


– Für Angehörige i.S. v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürfen nicht ungeschützt bleiben.

– Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i. S. v. § 52 StPO sind, sollte insoweit ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bleibt der Kernbereich teilweise ungeschützt.

Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürfen nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht – wie im Entwurf vorgesehen – auf Beweiszwecke begrenzt werden.

Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnungüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.

Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.

Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.

Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.


Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100g, 100h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10 200 (2002) auf 40 000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.


Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Akten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.
Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnungüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z. B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formellhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht-rückwirkend die formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 Prozent der Abfragen erfolgreich.


5.2 Bundesmeldegesetz – Zentralregister als zentrales Problem

Das BMI hat einen Referentenentwurf zum Bundesmeldegesetz (BMG) mit einem zentralen Bundesmelderegister (BMR) vorgelegt. Der Bedarf für ein zusätzliches umfangreiches zentrales Melderegister auf Bundesebene ist jedoch nicht belegt. Unabhängig davon muss die datenschutzrechtliche Position der Meldepflichtigen insgesamt verbessert werden.


– Beschränkung der Aufgaben der Meldebehörden auf den Identitätsnachweis,
– schlanker, gesetzlich festgelegter Merkmalskatalog,
– strenge Zweckbindung der über die Grunddaten hinausgehenden Angaben,


Ein BMR, das die Daten sämtlicher Einwohner enthält, würde erheblich tiefer in den Datenschutz eingreifen als die bestehenden dezentralen Register, insbesondere weil die Auswirkungen eines eventuellen Datenmissbrauchs erheblich größer wären. Zudem würde ein BMR die Möglichkeit eines direkten Zugriffs auf sämtliche Melderegisterdaten und ihre Verknüpfung mit anderen Dateien ermöglichen. Da das BMR die kommunalen Register nicht ersetzen, sondern nur ergänzen soll, muss für jedes in das BMR aufzunehmende Merkmal der Nachweis geführt werden, dass seine Speicherung in einer bundesweiten Datei erforderlich ist.


Ich halte den Referententwurf auch unter weiteren Aspekten für verbesserungsbedürftig:


– Die datenschutzrechtliche Position der Meldepflichtigen muss gestärkt werden, indem bestehende bloße Widerspruchsrechte (z. B. gegen Melderegisteraus-
künfte an Parteien zur Wahlwerbung oder an Adressbuchverlage) durch das Erfordernis einer vorherigen Einwilligung in die entsprechende Datenübermittlung ersetzt werden.

- Unbefriedigend ist auch die sog. einfache Melderegisterauskunft, die praktisch keinerlei Einschränkungen unterliegt. Der Meldepflichtige kann zur Zeit – von wenigen gesetzlichen Ausnahmeregulierungen abgesehen – nicht verhindern, dass seine Grunddaten an jedermann herausgegeben werden. Ich halte daher an meiner Forderung fest, als Korrektiv zumindest ein generelles Widerspruchsrecht des Betroffenen gegen einfache Melderegisterauskünfte einzuführen, weil es sich hier um Daten handelt, die zwangsläufig beim Bürger und primär zur Erfüllung hoheitlicher Aufgaben erhoben werden (vgl. 18. TB Nr. 5.7).

- Die Auskunftsrechte der Betroffenen gegenüber der Meldebehörden sollten gestärkt werden. Die Betroffe-

nen können nicht erkennen, an welche Stellen Melde-
daten fließen. Sie sollten daher die Möglichkeit erhal-
ten zu erfahren, welche Datenübermittlungen im Einzelfall stattgefunden haben und welche öffentlichen
und privaten Stellen Melderegisterauskünfte über sie eingeholt haben. Das bestehende Auskunftsrecht über regelmäßige Datenübermittlungen an andere Stellen sollte entsprechend ergänzt werden.

- Die seit langem erhobene Forderung nach der Ab-

schaffung der allgemeinen Hotelmeldepflicht bleibt aktuell (vgl. etwa 8. TB Nr. 2.2 und 19. TB Nr. 7.3). Die mit der Hotelmeldepflicht verbundene millionen-

fache Datenerhebung ist unverhältnismäßig. Hotelgäste können nicht schlechthin als Gefahrenquellen
oder potentielle Straftäter angesehen werden.

Ob es in der laufenden Legislaturperiode noch zu der vom BMI angestrebten Reform des Melderechts kommt, war zu Redaktionsschluss offen.

**5.3 Neue Ansätze in der amtlichen Statistik**

*Die statistische Datenerhebung und -aufbereitung bein-
den sich im Wandel und erfordern Flexibilität auf Seiten
des Datenschutzes.*

In der amtlichen Statistik vollzieht sich seit einiger Zeit ein tief greifender Wandel, der sowohl die Datenerhe-

bungsprozesse als auch die Aufbereitung der statistischen Daten und deren Nutzungsmöglichkeiten betrifft.

So gibt es eine deutliche Tendenz zu einer immer stärk-
eren Nutzung der in Verwaltungsregistern vorgehaltenen Datenbestände an Stelle von Befragungen der Betroffe-
nen, also weg von der Primärerhebung hin zur Sekun-
därerhebung. Etwa sollen bei dem Zensus 2011 die Erhe-

bungsdaten zu einem großen Teil aus verschiedenen Verwaltungsregistern gewonnen werden (vgl. hierzu Nr. 5.5). Die Hinwendung zu dieser „sekundären“ Daten-
erhebung wird vor allem mit der Entlastung der von sta-

tistischen Erhebungen betroffenen Bürger und der Not-
wendigkeit von Kosteneinsparungen begründet.

Dabei kann man nicht von vorneherein sagen, dass eine der beiden Methoden datenschutzfreundlicher sei. Bis-

weilen wird gegen statistische Primärerhebungen ange-

führt, dass der hiermit verbundene Eingriff größer sei als bei einer Sekundärerhebung, da ja bei letzterer keine „neuen“ Daten erhoben würden. Dies ist nur bedingt richt-

ig. Bei einer Sekundärerhebung werden Daten genutzt und zusammengeführt, die im Regelfall für andere Zwe-

cke erhoben wurden. Sekundärerhebungen gehen deshalb ganz überwiegend mit Zweckänderungen einher. Die Be-

troffenen „merken“ zudem nichts davon, dass ihre zu-

nächst für ganz andere Zwecke angegebenen Daten in einem neuen Zusammenhang verwendet werden. Sie kön-

nen also auch die Rechtmäßigkeit der Erhebung nicht selbst prüfen oder den Vorgang der Erhebung beeinflus-

sen. Damit wird von dem datenschutzrechtlichen Grund-

satz abgewichen, dass personenbezogene Daten beim Be-

troffenen mit seiner Kenntnis zu erheben sind. Einen
gewissen Ausgleich bietet die auch bei Sekundärstatisti-

ken notwendige bundesgesetzliche Grundlage, in der

schutzwürdige Belange der Bürger unter Wahrung des

Grundsatzes der Verhältnismäßigkeit berücksichtigt wer-

den müssen. Schließlich setzen umfangreichere Sekun-
därstatistiken – zum Beispiel die für 2011 geplante Volks-
zählung – voraus, dass die Daten aus unterschiedlichen Quellen zusammengeführt werden können, wofür eine entsprechende Infrastruktur benötigt wird. Es besteht immer die Gefahr, dass diese, für die Durchführung der sta-

tistischen Erhebung eingerichtete Infrastruktur entgegen der ursprünglichen Intention auch für die Zusammenfüh-

rung von Datenbeständen außerhalb der Statistik verwend-

et werden kann, mit möglicherweise erheblichen Folgen für die Betroffenen.

In Politik, Wirtschaft und Wissenschaft wächst das Inte-

resse an tiefer gegliederten, detaillierteren Informationen. Einzelangaben sollen deshalb gegebenenfalls in ihrer Ver-

änderung im Zeitablauf betrachtet werden. Dies bedeutet aber, dass sie auch längerfristig auf den Betroffenen rück-

führbar sind. Während es in der traditionellen statisti-

ischen Auswertung regelmäßig um Datenaggregate geht, die grundsätzlich nicht personenbeziehbar sind, handelt es sich bei diesem Ansatz um eine Ergänzung statistischer Aggregate um die Dokumentation des Verhältnisses der ein-

zelnen Erhebungseinheiten (Haushalte, Unternehmen) auf der so genannten „Mikroebene“.

Dieser Methodenwechsel ist aus datenschutzrechtlicher Sicht mit einem erheblichen Risiko behaftet, da hier eine wirksame Anonymisierung, die einen Rückschluss auf eine identifizierbare statistische Erhebungseinheit zumin-

dest faktisch ausschließt, kaum möglich erscheint. Dar-

über hinaus steht eine längerfristige Speicherung perso-

nenbezogener Einzelangaben im Konflikt mit dem vom Bundesverfassungsgericht in seinem Volkszählungsurteil von 1983 herausgearbeiteten Grundsatz der möglichst früh-

zeitigen Anonymisierung im Bereich der amtlichen Sta-

tistik. Eine umfassende, auf Dauer bestehende, aus den unterschiedlichsten Quellen gespeiste und fortgeschrie-

bene Mikro-Datensammlung dürfte daher unzulässig sein. Unterhalb dieses umfassenden Ansatzes kann aller-
dings die Verwendung von Mikrodaten durchaus mit den verfassungsrechtlichen Anforderungen vereinbar sein (s. u. Nr. 5.4).

5.4 KombiFiD

Ein Beispiel für den beschriebenen Methodenwandel bei Erhebung und Auswertung statistischer Daten ist das Projekt „KombiFiD – Kombinierte Firmendaten für Deutschland“.


Bei KombiFiD ist als Rechtsgrundlage der geplanten Datenverarbeitungsprozesse die schriftliche Einwilligung der betroffenen Unternehmen nach einer umfassenden Aufklärung über das Projekt vorgesehen. Dagegen habe ich keine grundsätzlichen Bedenken. Die Studie befindet sich derzeit noch in der Anfangsphase. Im weiteren Verlauf wird darauf zu achten sein, dass bei der Zusammenführung der Daten die für die jeweiligen Verwaltungsbereiche geltenden Geheimhaltungsbestimmungen beachtet werden. Eine Speicherung wird nur in einem jeweils abgeschotteten Forschungsbereich bei den Statistischen Ämtern, beim IAB und der Deutschen Bundesbank erfolgen.

5.5 Volkszählung 2011

Die Volkszählung 2011 wirft ihre Schatten voraus. Das hierfür vorgesehene neue Verfahren besteht aus einer Kombination von Registerzusammenführungen und Befragungen, so dass der überwiegende Teil der Bevölkerung durch die Erhebungen nicht direkt in Anspruch genom


5.5.1 Gesetzliche Vorgaben


Leider war ich bei der Erarbeitung dieser Änderung nicht beteiligt worden. Ich werde meine Bedenken im parlamentarischen Verfahren geltend machen.

**Kasten a zu Nr. 5.5.1**

**Die Zensuserhebungen nach dem geplanten ZensG 2011** bestehen aus folgenden Komponenten:

- Auf den Stichtag 9. Mai 2011 bezogene Zusammenführung und Auswertung der Daten der Meldebehörden, der Bundesagentur für Arbeit und von Dateien zum Personalbestand der öffentlichen Hand
- Postalische Befragung der rund 17,5 Mio. Gebäude- und Wohnungseigentümer zur Gewinnung von Wohnungs- und Gebäudedaten
- Stichprobenerhebungen bei ca. 8 Prozent der Bevölkerung zur Gewinnung aus den Registern nicht entnehmbarer erwerbs- und bildungsstatistischer Daten
- Befragung der Verwalter oder Bewohner von Gemeinschaftsunterkünften wie Anstalten, Wohnheimen und ähnlichen Einrichtungen (sog. Sonderbereiche)

Hinsichtlich der Merkmale hält sich der Entwurf strikt an die Vorgaben der EU-Zensusverordnung. Die Erhebung von über die Anforderungen der EU-Zensusverordnung hinausgehenden Merkmalen, wie der oben erwähnten klima- und energiepolitischen Merkmale oder auch der Religionszugehörigkeit, ist nach dem Entwurf des ZensG 2011 nicht vorgesehen (näheres s. Kasten b zu Nr. 5.5.1).

**Kasten b zu Nr. 5.5.1**


5.5.2 Stand der Vorbereitungen


5.6 Novellierung des Bundesarchivgesetzes

Die Übernahme laufend aktualisierter digitaler Daten in staatliche Archive wirft schwierige datenschutzrechtliche Fragen auf.

Archive verkörpern – mehr als alle anderen Institutionen – das gesellschaftliche Langzeitgedächtnis. Öffentliche Stellen des Bundes haben ihre nicht mehr benötigten Ak-

Der Übergang zu digitalen Verarbeitungsverfahren in der öffentlichen Verwaltung stellt die Archive vor erhebliche Herausforderungen. So muss entschieden werden, wie zukünftig mit elektronischen Registern (etwa dem Ausländerezentralregister oder dem Bundeszentralregister) umgegangen werden soll.

Ein Referentenentwurf des BMK, der sich zur Zeit noch in der Ressortabstimmung befindet, sieht für die laufend aktualisierten digitalen Aufzeichnungen vor, dass das Bundesarchiv zu bestimmten mit der zuständigen Behörde festzulegenden Stichtagen Kopien aller Registerinhalte übernimmt. Dies wäre datenschutzrechtlich nicht akzeptabel.

Schon nach der bisherigen Fassung des Bundesarchivgesetzes (BArchG) war die Übernahme von digitalen Daten trägern („maschinell lesbare Datenträger“ nach § 2 Absatz 5 Satz 2 BArchG) ausdrücklich vorgesehen. Dies ist etwa bei elektronischen Akten auch kein Problem, wenn dafür die bei traditionellen Akten verwendeten Verfahren angewandt werden. Die archivrechtliche Besonderheit der fortlaufend aktualisierten Register und sonstigen digitalen Dateien besteht nun darin, dass der archivrechtlich traditionell vorgesehene Archivierungszeitpunkt, der Zeitpunkt also, an dem die Unterlagen zur Erfüllung der behördlichen Aufgaben nicht mehr benötigt werden (§ 2 Absatz 1 Satz 1 BArchG), niemals eintritt. Diese Dateien werden laufend aktualisiert, also neue Bestände hinzugefügt und alte gelöscht. Sie werden zur Aufgabenerfüllung ständig benötigt. Die Vertreter der Archive halten es für fachlich geboten, diese Aufzeichnungen in Querschnittsproben der Nachwelt, insbesondere die vorgesehenen umfassenden Speicherungen für die Archivwürdigkeit. Schon aus Platzgründen wird nur ein geringer Teil der Unterlagen in das Bundesarchiv übernommen; der Rest wird zur Vernichtung freigegeben. Soweit die archivierten Materialien personenbezogen sind – etwa Personalakten – sorgen Datenschutz- und Löschungsregelungen für die Wahrung des Rechts auf informationelle Selbstbestimmung der Betroffenen.

Der Übergang zu digitalen Verarbeitungsverfahren in der öffentlichen Verwaltung stellt die Archive vor erhebliche Herausforderungen. So muss entschieden werden, wie zukünftig mit elektronischen Registern (etwa dem Ausländerezentralregister oder dem Bundeszentralregister) umgegangen werden soll.

EinReferentenentwurf des BMK, der sich zur Zeit noch in der Ressortabstimmung befindet, sieht für die laufend aktualisierten digitalen Aufzeichnungen vor, dass das Bundesarchiv zu bestimmten mit der zuständigen Behörde festzulegenden Stichtagen Kopien aller Registerinhalte übernimmt. Dies wäre datenschutzrechtlich nicht akzeptabel.

Schon nach der bisherigen Fassung des Bundesarchivgesetzes (BArchG) war die Übernahme von digitalen Datenträgern („maschinell lesbare Datenträger“ nach § 2 Absatz 5 Satz 2 BArchG) ausdrücklich vorgesehen. Dies ist etwa bei elektronischen Akten auch kein Problem, wenn dafür die bei traditionellen Akten verwendeten Verfahren angewandt werden. Die archivrechtliche Besonderheit der fortlaufend aktualisierten Register und sonstigen digitalen Dateien besteht nun darin, dass der archivrechtlich traditionell vorgesehene Archivierungszeitpunkt, der Zeitpunkt also, an dem die Unterlagen zur Erfüllung der behördlichen Aufgaben nicht mehr benötigt werden (§ 2 Absatz 1 Satz 1 BArchG), niemals eintritt. Diese Dateien werden laufend aktualisiert, also neue Bestände hinzugefügt und alte gelöscht. Sie werden zur Aufgabenerfüllung ständig benötigt. Die Vertreter der Archive halten es für fachlich geboten, diese Aufzeichnungen in Querschnittsproben der Nachwelt, insbesondere die vorgesehenen umfassenden Speicherungen, zu erhalten.


chert werden, dass sie nicht ohne weiteres miteinander verknüpft werden können.

Jede Vervielfältigung und Übermittlung personenbezogener Daten stellt für sich genommen bereits einen Eingriff in das Grundrecht dar, der aus meiner Sicht auch durch das wissenschaftliche Interesse nicht zu recht fertigen ist. Im Übrigen würde durch diese Form der Archivierung die in dem Referentenentwurf des BMK enthaltene datenschutzrechtliche Grundregel unterlaufen, dass Rechtsvorschriften über die Verpflichtung zur Vernichtung von Unterlagen der Archivierung vorgehen.

Es müssen also Lösungen gefunden werden, die sowohl archiv- als auch datenschutzrechtlichen Positionen gerecht werden. Eine vollständige, ungeprüfte Übernahme der Daten aus fortlaufend aktualisierten Registern lehne ich ab.

5.7 Zentrale Einlader- und Warndatei


Es bleibt abzuwarten, ob das Vorhaben noch in dieser Legislaturperiode auf den Weg gebracht werden kann. Bei Redaktionsschluss war das Gesetzgebungsverfahren jedenfalls noch nicht abgeschlossen.

5.8 Die Bundesbeauftragte für die Unterlagen des Staats sicherheitsdienstes der ehemaligen DDR (BStU)

Neben den Anträgen auf Akteneinsicht stellt die Verwendung der Unterlagen für die politische und historische Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes oder der Herrschaftsmechanismen der ehemaligen DDR einen meiner Kontrollschwerpunkte dar.

Als Ergebnis zweier Beratungs- und Kontrollbesuche bei Außenstellen der BStU kann ich erneut festhalten, dass die Mitarbeiter der BStU sich durch Sensibilität und Gewissenhaftigkeit im Umgang mit den personenbezogenen Daten auszeichnen.


5.9 Dopingbekämpfung

Auch bei der Dopingbekämpfung darf der Datenschutz nicht vernachlässigt werden.


Ich stehe mit dem BMI und der Nationalen Anti-Doping-Agentur (NADA) im Kontakt, um die entsprechenden Belange des Datenschutzes auch in weiteren europäischen Gremien zu unterstützen und verstärkt in die nationale Anti-Doping-Diskussion einzugreifen.
Zur Datenbank ADAMS

Nach dem Welt-Anti-Doping-Code sind die Athleten verpflichtet, vierteljährlich genaue und vollständige Angaben darüber zu machen, wo sie im kommenden Quartal wohnen, trainieren und an Wettkämpfen teilnehmen werden, sowie Änderungen unverzüglich anzusehen, damit sie jederzeit für Dopingkontrollen erreichbar sind. Spitzensportler müssen seit 1. Januar 2009 dafür hinaus für jeden Tag eine Stunde benennen, zu der sie sich an einem vorher angegebenen Ort für Dopingkontrollen bereit halten.

6 Elektronische Identität


Bereits in früheren TB habe ich Vorschläge zum Identitätsmanagement (IDM – s. Kasten a zu Nr. 6) veröffentlicht, z. B. im 21. TB Nr. 4.4, 4.13 oder 20. TB Nr. 4.1.1.

Durch die Verwendung von Chipkarten und durch die Nutzung des Internets hat die Frage von bewusster Anonymität bzw. bewusstem Umgang mit Kennungen, die die eigene Person identifizieren, z. B. mit E-Mail-Adressen, eine neue und zuvor nie gekannte Komplexität erreicht.

Besonders im Internet werden häufig viele unterschiedliche und kurzelebige Kennungen verwendet. Die Anwendungsbreite reicht von der Einrichtung verschiedener E-Mail-Adressen für unterschiedliche Zwecke bis zu einer eher spielerischen Verschleierung der eigenen Identität in Foren oder Chats. Daneben spielen Prozesse und Fragen der Anonymität und der Identifizierbarkeit im Internet aber auch bei Anwendungen im elektronischen Geschäftsverkehr oder im E-Government eine wichtige Rolle.

Das Identitätsmanagement (IDM) bezeichnet den geordneten und optimierten Umgang mit (unterschiedlichen) Identitätsdaten sowie mit Anonymität und Pseudonymen. Es umfasst die Verwaltung der Information über diese Identitäten, die Verwaltung der Authentifizationsnachweise, die Verwaltung der Berechtigungsstrukturen, die mit einer Identität verknüpft sind und die Protokollierung dieser Aktivitäten.


— die sichere Verwaltung von Identitäten,

— den Identifikationsprozess einer Einheit (inkl. optionaler Authentisierung) und

— die Information, die mit der Identifikation einer Einheit innerhalb eines bestimmten Kontextes verbunden ist.

In vielerlei Hinsicht können Identitätsmanagementsysteme problematisch sein. Mit Hilfe dieser Systeme müssen Nutzerinnen und Nutzer die vollständige Kontrolle über ihre Daten erhalten. Dort wo Anonymität oder pseudonyme Nutzungsarten angeboten werden, darf die Zusammenführung dieser Daten nicht ungewollt zu weiter gehender Identifizierung führen.


In den vergangenen Jahren hat die missbräuchliche Nutzung der Identitätsdaten einer natürlichen Person durch Dritte (Identitätsdiebstahl) deutlich zugenommen. Die am häufigsten auftretenden Formen von Identitätsdiebstahl sind Kreditkartenbetrug, Kontenraub und Bankbetrug; dabei wird für diese Diebstähle immer öfter das Internet genutzt. Dies machen auch jüngste Beispiele aus der Telekommunikationsbranche wieder deutlich.

Elektronischer Handel und elektronische Verwaltungsdiestleistungen werden von Bürgerinnen und Bürgern jedoch nur akzeptiert, wenn ihre Daten gegen Missbrauch und unrechtmäßige Kenntnisnahme geschützt sind. Hierzu gehört auch der Schutz vor Identitätsmissbrauch, etwa bei Bestellungen über das Internet. Gleich-
zeitig ist sicherzustellen, dass bei der Nutzung möglichst wenig personenbezogene Daten preisgegeben werden. Auch ist darauf zu achten, dass die „informationelle Gewaltenteilung“ bestehen bleibt, also die Trennung der zwischen den von verschiedenen Verwaltungsbereichen für unterschiedliche Zwecke erhobenen Daten (s. Kasten b zu Nr. 6). Eindeutige Authentifizierung und Datenvermeidung stehen dabei nicht in einem unauflosbaren Widerspruch, denn intelligente Authentifizierungsmechanismen kommen ohne übergreifende Identifikationsnummern und Personenkennzeichen aus. Durch ein modernes Identitätsmanagement können sowohl der Datenschutz als auch die Informationssicherheit gewinnen.

Kasten b zu Nr. 6

Daten- und Verbraucherschutz halten folgende Mindestforderungen beim Identitätsmanagement (IDM) für notwendig:

- selbstständige Verwaltung und Kontrolle der Verwendung von Identitätsdaten durch die Nutzer,
- den jeweiligen Erfordernissen angepasste und abgestufte Nutzungsmöglichkeiten auch hinsichtlich Anonymität und Authentizität,
- sichere Authentifizierung auch auf der Anbieterseite,
- Vermeidung von zentralen Verfahren und der Möglichkeiten zur Zusammenführung von Identitätsdaten,
- Einführung von Benachrichtigungspflichten bei Datennässen und -verlusten.

6.1 Elektronische Gesundheitskarte

Die elektronische Gesundheitskarte wird später als vorgesehen kommen. Die lange Verzögerung ruft aber Konkurrenten auf den Plan, die alternative Modelle von elektronischen Gesundheitsakten auf dem Markt anbieten.


Der Basis-Rollout hat begonnen


Kasten zu Nr. 6.1

Zwiebelschalenmodell des Basis-Rollouts; die Zahlen geben den zeitlichen Ablauf wieder.

Bild entnommen aus einem Vortrag von D. Drees/gematik beim Euroforum am 20. Mai 2008

Zunächst wird die Gesundheitskarte im Unterschied zur bisherigen Krankenversichertenkarte ein Lichtbild enthal-
ten und nur im Offline-Betrieb eingesetzt. Sie kann zwar schon die Basisfunktionen Versichertenstammdatendienst, elektronisches Rezept und Notfalldatensatz bedienen, was teilweise nur im Online-Betrieb geht. Voraussetzung hierfür ist das Vorhandensein eines Heilberufsausweises bei den Leistungserbringern und eine funktionierende Telematikinfrastruktur. Diese schrittweise Migration ist der bisherigen Testergebnissen geschuldet, die die erheblichen Sicherheitsanforderungen und die Komplexität der Infrastruktur aufzeigten.


Nach dem aktuellen Konzept der gematik werden die schützenswerten Daten in einer Region dann in den geschützten Bereich der elektronischen Gesundheitskarte überführt, wenn sowohl in dieser Region als auch in den angrenzenden Regionen eine Anbindung von 95 Prozent aller Leistungserbringer am Online-Betrieb gegeben ist. Das BMG hat zugesagt, dass die Speicherung und Nutzung dieser Daten auf der Krankenversicherungskarte ab diesem Zeitpunkt nicht mehr zulässig ist. Die bis dahin noch offenen Daten auf der Gesundheitskarte sind ebenfalls zu löschen.

Wahrung von Versichertenrechten


6.1.1 Patientendaten im Internet – Welche Risiken verbergen sich hinter den elektronischen Gesundheitsakten und der elektronischen Fallakte?

Eine große deutsche Krankenkasse bietet ihren Mitgliedern im Rahmen eines Forschungsprojektes an, ihre Gesundheitsdaten im Internet über eine so genannte elektronische Gesundheitsakte zu führen. In dieser Akte können alle persönlichen gesundheitsrelevanten Informationen abgelegt, verwaltet und jederzeit von überall mit Hilfe eines Internet-Zugangs abgerufen und eingesehen werden. Notizen über Arztbesuche, Röntgenbilder, Arztbefunde, Diagnosen, Therapien, verordnete Medikamente: Kurzum alles, was über den Gesundheitzustand des Nutzers Aufschluss gibt, ist damit per Internet verfügbar. Dabei werden medizinische Daten ge-
speichert, die gemäß § 3 Absatz 9 BDSG besonders schützenswert sind. Dementsprechend müssen datenschutzrechtliche Forderungen wie die Datenhoheit des Versicherten, die Freiwilligkeit der Teilnahme sowie das Erforderlichkeitsprinzip als Maßstab angelegt werden. Bei der Gesundheitsakte ist im Hinblick auf die Freiwilligkeit problematisch, dass diese Akte in der Regel durch die Krankenkasse finanziert wird und mit Pflichten des Versicherten verbunden ist. Deswegen wird die Krankenkasse versucht sein zu sehen, ob sich der Versicherte auch an die Bedingungen der integrierten Versorgung und die damit verbundenen Pflichten hält, indem sie den Bestand der Akte, Nutzunggrad und Effizienz der Behandlungen unter die Lupe nimmt. Ich werde das Forschungsprojekt der Krankenkasse kritisch begleiten und auch ähnliche Verfahren, die von Softwarefirmen entwickelt und angeboten werden, beobachten.

Daneben werben verschiedene kommerzielle Anbieter seit Monaten z. B. in den USA für Programme, die persönliche Patientendaten im Internet speichern und mit medizinischen Informationen verständlicher machen sollen. Es dürfte nur eine Frage der Zeit sein, bis diese Internet-Gesundheitsakten auch in Deutschland verfügbar sind.


6.1.1.2 Die elektronische Fallakte

Daneben ist im Bereich der medizinischen Versorgung als weitere Variante die elektronische Fallakte im Gespräch. Bei der elektronischen Fallakte handelt es sich um einen Werkzeug für eine sektorenübergreifende Kommunikation zwischen einzelnen Leistungserbringern. Sie soll nur für konkrete Behandlungsfälle angelegt werden und für eine bessere Kommunikation zwischen dem jeweiligen Krankenhaus und dem ambulanten behandelnden Arzt sorgen.


6.1.2 Status „Sozialhilfeempfänger“ auf der Krankenversichertenkarte


In verschiedenen Stellungnahmen haben die Kassenärztliche Bundesvereinigung (KBV) sowie der Spitzenverband der gesetzlichen Krankenversicherung (GKV), die gemeinsam die „Technischen Spezifikationen der Versicher-

Diese nachvollziehbare Begründung hat mich dazu veranlasst, meine datenschutzrechtlichen Bedenken einstweilen zurückzustellen. In der Zukunft wird sich das Problem mit der Ablösung der Krankenversichertenkarte durch die elektronische Gesundheitskarte in dieser Weise nicht mehr stellen, da die neue Karte die Angaben nach § 291 Absatz 2 SGB V dazu gehört auch das Statusmerkmal „Sozialhilfeempfänger“ in verschlüsselter Form enthalten wird. Das Ziel, kurzfristig eine datenschutzrechtliche Bedenken einstweilen zurückzustellen zu können, ist erreicht, denn die Krankenkassen müssen die entsprechenden Kosten den Trägern der Sozialhilfe oder der öffentlichen Jugendhilfe gemäß § 264 Absatz 7 SGB V in Rechnung stellen.

6.2 Die Einführung des elektronischen Entgeltnachweises (ELENA) steht bevor

Nach jahrelangen Vorarbeiten hat die Bundesregierung einen Gesetzentwurf zum ELENA-Verfahren eingereicht. Im Rahmen der parlamentarischen Beratungen habe ich darauf hingewiesen, dass noch nicht alle datenschutzrechtlichen Bedenken vollständig ausgeräumt werden konnten.


6.3 Biometrie und Datenschutz


Mittlerweile wird eine Vielzahl von biometrischen Verfahren kommerziell genutzt, etwa Fingerabdruck-, Iris-, Venen-, Sprecher- oder Unterschriftenerkennung. Mit der stärkeren Verbreitung von Biometrie wächst das Missbrauchspotential, weil die derzeit häufig eingesetzten


Die im E-Pass und im E-Personalausweis gespeicherte Biometrie wird mangels vorhandener Kontrolltechnik derzeit noch nicht im Grenzkontrollverfahren eingesetzt.

Im Berichtszeitraum habe ich mich mit folgenden weiteren Anwendungen biometrischer Systeme befasst:

- **Grenzkontrollsyste**: zur Anwendungserprobung von Gesichtserkennungsverfahren (GANGes)

2009 will die Bundespolizei die Möglichkeiten der Gesichtserkennung im Projekt GANGes am Frankfurter Flughafen testen. GANGes soll im Rahmen der Grenzkontrolle zum Einsatz kommen, wobei ein aktuell aufgenommenes Foto mit dem im Ausweis gespeicherten Bild verglichen wird (s. auch Nr. 6.4). Dieses Verfahren soll der beschleunigten Kontrolle von Passagieren dienen und gleichzeitig die Hürde für einen Passmissbrauch erhöhen. Der Feldversuch hat zum Ziel, die Tauglichkeit des Verfahrens für eine automatisierte Grenzkontrolle zu überprüfen.

Bei einem erfolgreichen Test von GANGes soll das ABG-Verfahren – das bislang nur auf freiwilliger Basis stattfindet – als offizielles Verfahren abgelöst werden.

- **Fast Identification**


- **Foto-Fahndung**

Im Forschungsprojekt „Foto-Fahndung“ hat das BKA von Oktober 2006 bis Ende Januar 2007 die biometrische Gesichtserkennung als Fahndungshilfsmittel für die Polizei getestet (s. 21 TB Nr. 5.2.6). Im Ergebnis war es mit den getesteten Systemen nur dann möglich, gesuchte Personen in Menschenmengen automatisch wieder zu erkennen, wenn die äußeren Rahmenbedingungen, insbesondere die Beleuchtung, dies zuließ. Von der Einführung des Fahndungshilfsmittels hat das BKA vorerst abgesehen. Ich begrüße dieses bedachte Vorgehen (s. auch Nr. 8.1).

- **FIREBIRD**


### 6.3.1 Elektronischer Pass der II. Generation

*Der sog. E-Pass der II. Generation, der neben dem digitalisierten Lichtbild auch digitalisierte Fingerabdrücke enthält, ist eingeführt worden. Die datenschutzrechtliche Skepsis bleibt.*


Die Speicherung biometrischer Merkmale für staatliche Identitätskontrollen weckt zudem Begehrlichkeiten nichtöffentlicher Stellen. Ich halte es nur für eine Frage der Zeit, dass auch die Wirtschaft Interesse an einer biometrisch abgesicherten Identifizierung entwickelt und deshalb Zugriff auf die Biometriedaten im elektronischen Pass und im elektronischen Personalausweis (s. u. Nr. 6.3.2) verlangt. Unabhängig von diesem schon jetzt absehbaren Interesse der Wirtschaft stellt sich auch heute schon die Frage nach der Sicherheit der für die Aufnahme biometrischer Daten verwendeten Technik. Was geschieht, wenn kein hinreichender Kopierschutz der Daten (mehr) gewährt wird und Kriminelle „gestohlene“ Fingerabdruckdaten missbrauchen können?

Die Novellierung des Passgesetzes wird immerhin einigen zentralen Forderungen des Datenschutzes gerecht:


Der Ausleseprozess am „Chipterminal“ erfolgt in der Regel mit Kenntnis und in Gegenwart des Betroffenen, so dass jedenfalls hier ein gewisses Maß an Transparenz gewährleistet ist. Allerdings ist nicht völlig auszuschließen, dass die nur mit dem schwächeren Verfahren der „Basic Access Control“ (BAC) geschützten Daten des Gesichtsbildes von unberechtigten Dritten ausgelesen werden können.

Aus datenschutzrechtlicher Sicht würde ich es begrüßen, wenn ein (direkten) Online-Zugriff aller Polizei- und Ordnungsbehörden auf die bei den örtlichen Passbehörden gespeicherten Lichtbilder ausgeschlossen und eine datenschutzfreundliche Regelung für eine kontrollierbare Übermittlung gefunden werden könnte.

In der Vergangenheit hatten verschiedene Meldebehörden beim Passantragsverfahren datenschutzrechtliche Probleme. Diese wurden häufig durch organisatorische Mängel in den einzelnen Behörden hervorgerufen. Ob die Schwachstellen beim Antragsverfahren gänzlich behoben sind, werden die weiteren Kontrollen der für den Bereich zuständigen Landesbeauftragten für den Datenschutz zeigen.

6.3.2 Elektronischer Personalausweis


Der Elektronische Personalausweis (E-Personalausweis) sollte ursprünglich wie der E-Pass der II. Generation obligatorisch mit digitalisiertem Lichtbild und digitalisierten Abdrücken der beiden Zeigefinger ausgestattet werden. Darüber hinaus soll der E-Personalausweis optional einen elektronischen Identitätsnachweis und eine elektronische
Signaturfunktion nach dem Signaturgesetz ermöglichen. Der E-Personalausweis ist damit auch als einheitliches Werkzeug für verschiedene Formen verbindlichen, identitätsrelevanten Handelns im elektronischen Rechtsverkehr sowohl für E-Commerce als auch für E-Government konzipiert. Seine Funktionalitäten, aber auch die damit möglichen Risiken wie Missbrauch der ID-Funktion bzw. Identitätsdiebstahl, gehen somit deutlich über die des E-Passes hinaus.


Aus meiner Sicht sollte den Bürgerinnen und Bürgern eine zuverlässige und einfache Möglichkeit gegeben werden, die Richtigkeit der tatsächlich gespeicherten Daten zu überprüfen. Ich hoffe, dass die für eine solche IT-gestützte Verifikation erforderliche Technik für E-Personalausweis und E-Pass zeitnah beschafft und bundesweit in der Fläche verfügbar sein wird.

Mit der Verbreitung biometrischer Zugangssicherungsverfahren wird das Missbrauchsrisko steigen; Fälle des zumindest versuchten – Identitätsdiebstahles könnten zunehmen. Eine effektive Sicherung der biometrischen Daten auf dem E-Personalausweis ist deshalb unverzichtbar. Die Bundesregierung hat diese Forderung aufgegriffen und will diese Daten mit dem bereits beim E-Pass eingesetzten Zugriffsschutz (Extended Access Control) sichern.

Wegen der Zusatzfunktionen für die Bereiche des E-Commerce und des E-Government ergibt sich beim E-Personalausweis eine deutlich größere Missbrauchsfahrer als beim E-Pass.


Das so genannte Hinterlegungsverbot des § 1 Absatz 1 Satz 3 PauswG und die Verpflichtung des Ausweisinhabers, durch technische und organisatorische Maßnahmen zu gewährleisten, dass die Funktion des elektronischen Identitätsnachweises nur in einer sicheren Umgebung eingesetzt werden kann (§ 26 Absatz 3 PauswG) zeigen, dass die Bundesregierung die Missbrauchsfahrer ebenfalls erkannt hat.


6.4 Automatisierte Grenzkontrollen/Projekt GAnGes bzw. easyPass

Die Bundespolizei will ein neues Verfahren zur Durchführung der Grenzkontrolle unter Verwendung des biometrischen Merkmals des Gesichtsbildes testen. Am Flughafen Frankfurt/Main soll hierzu ein Pilotprojekt durchgeführt werden.

Neben der automatisierten biometriegestützten Grenzkontrolle (ABG), über die ich mehrfach berichtet hatte (s. 20. TB Nr. 5.3.5 und 21. TB Nr. 4.5.2; vgl. auch o. Nr. 6.3), erprobt die Bundespolizei ein weiteres biometrisches Verfahren zur Beschleunigung und Vereinfachung des Grenzkontrollprozesses. Hierfür soll das Gesichtsbild der Person, die ein Reisedokument zur Überprüfung vorlegt, herangezogen werden.

Im Rahmen des 2009 beginnenden Pilotprojektes „GAnGes“ (Grenzkontrollsystem für die Vermeidung von Identitätsnachweismitteln Verfahren) bzw. „easyPass“ am Flughafen Frankfurt/Main soll u. a. geprüft werden, ob sich der Einsatz von Identitätsnachweismitteln Verfahren in Bezug auf Erkennungsgenauigkeit und das zugrunde liegende Sicherheitsniveau, z. B. hinsichtlich der Täuschung- oder Überwindungsmöglichkeit, für die Grenzkontrolle eignet. Die Teilnahme am Test ist nur für EU-Bürger möglich, die über einen elektronischen Reisepass (E-Pass) verfügen, in dessen integriertem Speicherchip das Gesichtsbild der Passinhaberin bzw. des Passinhabers hinterlegt ist.

Für die Durchführung des Pilotprojektes soll ein Datenbe-

Auf meine Anregung hin haben das BMI und die Bundespolizei eine Einwilligungserklärung und ein Informationsblatt über die freiwillige Teilnahme am Pilotprojekt „easyPass“ erarbeitet. Reisende, die am GAnGes- bzw. easyPass-Verfahren nicht teilnehmen, durchlaufen das herkömmliche Verfahren am Grenzkontrollschalter der Bundespolizei.

Ich werde das Projekt weiterhin begleiten.

6.5 Bundesmeldegesetz


Das BMI beabsichtigt, nach der durch die Föderalismusreform im Jahre 2006 erfolgten Übertragung der Gesetzgebungskompetenz für das Melderecht auf den Bund, das Meldewesen gesetzlich umfassend neu zu regeln und ein Bundesmelderegister (BMR) einzurichten (zu grundsätzlichen Fragen und zur Historie s. Nr. 5.2).

Um die Persönlichkeitsrechte und den Schutz der Identität des Einzelnen zu gewährleisten, sind jedoch einige Funktionsbedingungen bei der Einrichtung eines BMR unerlässlich:


Das BMI hat erklärt, dass es ein Identitätsmanagement bei einer Reform des Meldewesens konzeptionell vorsehen und gesetzlich absichern wolle.

6.6 Bürgerportale: Elektronischer Königsweg zur Verwaltung?


Grundsätzlich begrüße ich diese Bemühungen. Zwar ermöglicht bereits die elektronische Signatur nach dem Signaturenrecht ein hohes Maß an Sicherheit. Leider sind
aber seit vielen Jahren die Angebote und Nutzungszenahlen bei der elektronischen Signatur nicht vorangekommen, so dass diese Infrastruktur bis heute nicht in ausreichender Breite zur Verfügung steht.

Kasten zu Nr. 6.6

**Bürgerportalgesetz**

Ziel des Entwurfs eines Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften ist,

- einen Rechtsrahmen zur Einführung vertrauenswürdiger Bürgerportale im Internet zu schaffen, der für Dienstanbieter Rechtssicherheit schafft und es ihnen ermöglicht, die Rechtsqualität der als Bürgerportaldienste erfassten Dienste im Internet zu steigern,

- für die elektronische Kommunikation im Rechts- und Geschäftsverkehr vertrauenswürdige Lösungen zu schaffen, bei denen sich die Teilnehmer der Sicherheit der Dienste, der Vertraulichkeit der Nachrichten und der Identität ihrer Kommunikationspartner sicher sein können,

- die Rechtssicherheit im elektronischen Rechts- und Geschäftsverkehr durch verbesserte Beweismöglichkeiten zu stärken,

- die Möglichkeiten elektronischer Kommunikation fortzuentwickeln, indem eine Zustellung und eine Bestätigung des Zugangs auch für elektronische Erklärungen ermöglicht wird,

- den (freiwilligen) Eintrag einer elektronischen Bürgerportaladresse in ein Melderegister ermöglicht und dadurch eine Möglichkeit der elektronischen Zugangseröffnung für alle Behörden zu schaffen.

Im weiteren Gesetzgebungsverfahren sind folgende wichtige Punkte noch zu verbessern:


4. Die Prüfung der Anbieter setzt Regelungen zur Gewährleistung eines hohen Datenschutzniveaus bei den Anbietern voraus. Die Mindestanforderungen für das Audit müssen einheitlich für alle Anbieter vorgegeben werden. Von daher bietet sich eine Verzahnung mit dem Entwurf zum Datenschutzauditgesetz an (s. auch unter Nr. 2.4).


**6.7 RFID (Radio Frequency Identification)**

Immer noch fehlt eine wirksame Selbstverpflichtung der Wirtschaft oder eine gesetzliche Regelung zum Einsatz von Funkchips.

Im letzten Tätigkeitsbericht (21. TB Nr. 4.3) habe ich bereits ausführlich über die RFID-Technologie, ihre Gefahren für die Persönlichkeitsrechte und die rechtlichen Möglichkeiten ihrer Begrenzung berichtet.

Der Bestandsaufnahme der Bundesregierung sowie den daraus gezogenen Schlussfolgerungen für den künftigen Handlungsbedarf kann ich grundsätzlich zustimmen. Die von den Datenschutzbeauftragten in Bund und Ländern erhobenen datenschutzrechtlichen Forderungen (vgl. 21. TB, Kasten zu Nr. 4.3) könnten auf diese Weise umgesetzt werden. Eine Selbstverpflichtung der Wirtschaft halte ich dann für akzeptabel, wenn dafür bestimmte Bedingungen erfüllt sind:


Sollten die Bedingungen nicht erfüllt sein, ist der Gesetzgeber gefordert, durch entsprechende Ergänzungen des Datenschutzrechts Abhilfe zu schaffen. Das Gleiche gilt erst recht, wenn eine Selbstverpflichtung nicht zustande kommt.

Auch auf europäischer Ebene wurde der Konsultationsprozess der Europäischen Kommission fortgesetzt. Der Europäische Datenschutzbeauftragte hat sich dabei ebenso wie andere Datenschutzbehörden aus Deutschland und Europa für die Schaffung gesetzlicher Regelungen ausgesprochen, die ein striktes Opt-in-Prinzip sowie die Förderung datenschutzfreundlicher Technologien vorschreiben.


7 Internet

7.1 Geoinformationen und Datenschutz


Datenschutzgerechter Zugang zu Geoinformationen


Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (Bundestagsdrucksache 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das UIG ist deshalb nicht angemessen und lässt die in der INSPIRE-Richtlinie vorgesehenen weiteren Möglichkeiten zum Schutz der Persönlichkeitsrechte unberücksichtigt (s. Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008, Kasten zu Nr. 7.1)

7.2 Ihr Haus im Internet?


Vergleichbare Daten sind zwar schon vor Jahren angeboten worden, allerdings per CD. Bereits damals haben sich hieran datenschutzrechtliche Diskussionen entzündet (vgl. 18. TB Nr. 31.3). Neu ist an „Street View“, dass diese Daten kostenlos weltweit online verfügbar gemacht werden sollen. Das hat erhebliche datenschutzrechtliche Auswirkungen.


Zudem kann eine Unkenntlichmachung technisch – mindestens derzeit – noch nicht vollständig umgesetzt werden. Google hat angekündigt, die in Aufnahmen dargestellten Personen sowie KfZ-Kennzeichen besser un-
kenntlich zu machen. Die bisher dazu eingesetzte Software funktioniert noch nicht fehlerfrei.


Kasten zu Nr. 7.2


Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet


Die Zehn Gebote für Betreiber sozialer Netzwerke

1. Beachten Sie die Vorgaben des Datenschutzrechts
2. Klären Sie Ihre Nutzer verständlich und offen über den Umgang mit ihren Daten auf
3. Geben Sie Ihren Nutzern mehr Kontrolle über die Verarbeitung Ihrer Profil- und Verkehrsdaten
4. Bieten Sie datenschutzfreundliche Standardeinstellungen an
5. Bessern Sie kontinuierlich die Sicherheit Ihrer Informationssysteme
6. Jedermann hat ein Recht auf Auskunft über seine personenbezogenen Daten in einem Netzwerk – egal ob er oder sie Mitglied ist oder nicht
7. Profile müssen einfach und vollständig zu löschen sein
8. Ermöglichen Sie die Nutzung Ihrer Dienste unter Pseudonym
9. Verhindern Sie, dass Profildaten Ihrer Nutzer von Dritten kopiert werden
10. Stellen Sie sicher, dass Daten Ihrer Nutzer von externen Suchmaschinen nur dann gefunden werden können, wenn die Betroffenen zuvor ausdrücklich eingewilligt haben


7.3 „Super Nanny“ Datenschutz?


7.4 Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums in Kraft


Es gewährt den Rechteinhabern, wie insbesondere der Musik- und Filmindustrie mit Blick auf „Piraterie“ in dem Internet-Tauschbörsen, nunmehr einen zivilrechtlichen Auskunftsanspruch gegen die Internet-Zugangsprovider, um mögliche Rechtverletzer zu ermitteln, § 101 Urheberrechtsgesetz (UrhG). Damit erübrigt sich das bisherige Vorgehen der Rechteinhaber, über das Akteurensichtrecht im strafrechtlichen Ermittlungsverfahren, § 406e StPO, an die Daten zur Identifizierung des Nutzers zu gelangen.


Gleiches gilt für den vielfach geforderten Rückgriff auf die sog. Vorratsdaten (vgl. Nr. 3.2.1) zur Auskunftserteilung an Rechteinhaber. Der Gesetzgeber hat bei der Umsetzung der Richtlinie zur Vorratsdatenspeicherung deren Verwendung ausdrücklich auf Zwecke der Strafverfolgung und der Gefahrenabwehr, § 113b Absatz 1 Satz 1 TKG, beschränkt. Damit ist aber eine Erstreckung auf zivilrechtliche Auskunftsansprüche, wofür sich im Gesetzgebungsverfahren noch der Rechtsausschuss des Bundesrates ausgesprochen hatte (Bundesratsdrucksache 798/1/07), ausgeschlossen. Durch die höchstrichterliche Begrenzung der derzeitigen Nutzung der auf Vorrat zu speichernden Daten auf schwere Katalogstraftaten gemäß § 100a Absatz 2 StPO (Beschluss des BVerfG vom 11. März 2008, 1 BvR 256/08), dürfte einer weiteren Diskussion in diese Richtung ohnehin die Grundlage entzogen sein.


Für diese Verwendung der Verkehrsdaten für Mahnungen „auf Zuruf“ der Rechteinhaber gibt es keine Rechtsgrundlage. Weder das TKG noch der o. g. zivilrechtliche Auskunftsanspruch in § 101 UrhG, der neben der richterlichen Anordnung offensichtliche Rechtsverletzungen im gewerblichen Ausmaß voraussetzt, erlaubt den Providern dieses Vorgehen zur Identifikation von Internet-Nutzern.

Auch ich kann das legitime Interesse der Musik- und Filmindustrie, gegen Urheberrechtsverletzungen im Internet vorzugehen, durchaus nachvollziehen. Die Mittel müssen aber verhältnismäßig sein, den Interessen der Rechtseinhaber und dem Schutz des Fernmeldegeheimnisses sowie sonstiger Verfassungsgüter also gleichermaßen Rechnung tragen.

7.5 Die Jobbörse als Internet-Angebot der Bundesagentur für Arbeit

Die Jobbörse stellt als Teil des „Virtuellen Arbeitsmarktes“ ein Verfahren der Arbeitsverwaltung dar, das nur durch das Internet ermöglicht wird.


7.6 Persönliche Daten im Fokus von Suchmaschinen

Der Datenschutz bei Suchmaschinen bleibt ein datenschutzrechtlicher Schwerpunkt.


Diese berechtigten Sorgen haben dazu beigetragen, dass der Datenschutz bei Suchmaschinen zu einem der wichtigsten Themen von nationalen und internationalen Da-

Mein Anliegen ist ein zumindest europaweit gültiger Datenschutzstandard für Suchmaschinen, der von allen Betreibern eingehalten wird und eine koordinierte Datenschutzaufsicht nach einheitlichen Kriterien ermöglicht.

Kasten zu Nr. 7.6

Anforderungen an Suchmaschinen

– Die Europäischen Datenschutzregelungen gelten auch für Suchmaschinen, die ihren Sitz außerhalb von Europa haben, ihren Dienst aber in Europa anbieten.

– Die EU-Richtlinie zur Vorratsdatenspeicherung (2006/24/EG, vgl. Nr. 3.2.1) gilt nicht für Suchmaschinen.


– Die Nutzer müssen über den Zweck der Datenverarbeitung sowie ihre Rechte auf Auskunft, Änderung und Löschung informiert werden.

– Die Verwendung der Daten für Nutzerprofile bedarf der Einwilligung des Betroffenen.

7.7 Ortung durch Handys und andere Gerätschaft

Die informationelle Selbstbestimmung schützt auch dar­ vor, dass Dritte (etwa Vorgesetzte oder Lebenspartner) heimisch und gegen den Willen der Betroffenen aufspüren können, wo man sich aufhält. Auch hier ist die moderne Technik schon einen Schritt weiter.


zur Notrufverordnung gelöst werden kann, bleibt abzuwarten. Außerdem muss der Wille von Nutzern respektiert werden, in bestimmten Fällen nicht präzise geortet zu werden. Hierfür müssen die erforderlichen technischen Voraussetzungen geschaffen werden, etwa die Möglichkeit, eine Satelliten-Ortungsfunktion im Handy bei Bedarf abzuschalten.

Ich bestehe nicht, dass Ortungsdienste in vielen Bereichen durchaus sinnvoll eingesetzt werden können. Umso wichtiger ist es, dass dabei die Privatsphäre der Nutzer gewahrt und Missbräuche unterbunden werden. Während andere schwere Eingriffe in den persönlichen Lebens- und Geheimbereich bereits strafrechtlich erfasst sind, etwa die Verletzung der Vertraulichkeit des Wortes oder heimliche Bildaufnahmen (§§ 201, 201a StGB), besteht durchaus soweit als möglich begründete Möglichkeit, eine Satelliten-Ortungsfunktion im Handy bei Bedarf abzuschalten.

7.8 Verwendung von Telekommunikationsverkehrsdaten für Straßenverkehrsinformationen

Telekommunikationsverkehrsdaten enthalten auch Informationen, die für ganz andere Zwecke interessant sein können.

Verkehrsdaten sind für Telekommunikationsunternehmen ein wertvolles Gut – nicht nur für Abrechnungszwecke. Anders als im Festnetz fallen beim Internet-Zugang oder im Mobilfunkbereich weitaus mehr Verkehrsdaten an, die auch von wirtschaftlichem Interesse sind. So möchten etwa einige Firmen das Surfverhalten von Internet-Nutzern auswerten, um genauere Erkenntnisse über das allgemeine Nutzerverhalten zu gewinnen oder den Nutzern gezielte Werbung zu präsentieren. Alle Modelle, die mir hierzu bisher bekannt sind, gehen jedoch weit über das hinaus, was in Deutschland zulässig ist.


In der Telekommunikation unterscheidet man folgende Arten von Daten:

Bestandsdaten sind Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Hierzu gehören etwa Name, Adresse, Kontonummer. Es besteht eine Pflicht, für Abfragen von Sicherheitsbehörden bestimmte Bestandsdaten zu erheben, auch wenn diese betrieblich nicht erforderlich sind (s. § 111 TKG). Ein unachtsamer Umgang mit diesen Daten (s. Nr. 3.2.4) oder eine missbräuchliche Nutzung z. B. von Kontendaten kann schwerwiegende Folgen für den Teilnehmer haben.

Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden und unterliegen dem Fernmeldegeheimnis (Artikel 10 GG, § 88 TKG). Dies sind neben den Daten, die man vom Einzelverbindungsnachweis kennt, auch Standortdaten bei Handygesprächen oder IP-Adressen beim Abruf von E-Mails. Auch hier besteht eine Pflicht zur Vorratsdatenspeicherung (s. Nr. 3.2.1). Die Aussagekraft dieser Daten ist sehr hoch, da soziale Netzwerke oder Bewegungsprofile erkennbar werden. Den Wert dieser Daten hatte auch die Sicherheitsabteilung eines großen Telekommunikationsdiensteanbieters erkannt (s. Nr. 3.2.2). Auch die temporär anfallende Signalisierung für den Netzbetrieb zählt zu den Verkehrsdaten und kann für andere Zwecke interessant sein (s. Nr. 7.8). Bei bestimmten Interessenlagen ist die Definition von Verkehrsdaten jedoch auslegungsfähig (s. Nr. 7.11).

Der Inhalt der Telekommunikation, also etwa das Telefongespräch, der Text einer SMS oder E-Mail oder übertragene Daten unterliegen ebenso dem Fernmeldegeheimnis und genießen den höchsten rechtlichen Schutz. Erfreulicherweise muss sich der BfDI weniger häufig mit Datenschutzproblemen zum Inhalt der Telekommunikation beschäftigen, ein Fall findet sich im 20. TB (Nr. 13.2.1).
7.9 Von der Schwierigkeit, Gesetze anzuwenden, am Beispiel des Telemediengesetzes


Angesichts dieser Situation halte ich einen verbindlichen Leitfaden zur rechtskonformen Verarbeitung von Nutzungsdaten für die Bundesbehörden für erforderlich.


Was die Verarbeitung für statistische Zwecke betrifft, soll jedoch alles beim Alten bleiben. Deshalb kann ich den Website-Anbietern nur raten, die Nutzungsdaten vor der Auswertung in geeigneter Weise zu anonymisieren, wie das auch bei den Besucherdaten meiner eigenen Website geschieht. Auch wenn dadurch das Ergebnis der Auswertung ein wenig verzerrt wird, reichen die anonymen Daten zur Optimierung des Internet-Angebots aus.

7.10 Homepage-Überwachung durch das Bundeskriminalamt

Das BKA hat die Zugriffe auf veröffentlichte Fahndungs ausschreibungen auf seiner Website erfasst. Die Maßnahme wurde inzwischen eingestellt, da ich das BMI und das BMJ von der Rechtswidrigkeit der Erhebung überzeugen konnte.

Im Berichtszeitraum habe ich geprüft, in welcher Weise das BKA das Internet zur Erfüllung seiner Aufgaben nutzt. Dabei habe ich u. a. festgestellt, dass es die Erfassung der Zugriffe auf Fahndungs ausschreibungen, die auf seiner Website im Zusammenhang mit ungeklärten Straftaten veröffentlicht werden, als neue Fahndungsmaßnahme entwickelt hat.


Bei der Homepage-Überwachung werden Zugriffe auf Fahndungsseiten auf dem Webserver des BKA mit einem

Das BKA vertrat die Auffassung, dass diese Form der Homepage-Überwachung auf die Ermittlungsgeneralklause des § 163 StPO gestützt werden könne. Der Internet-Nutzer rechne außerdem damit, dass die Protokollation auf den Webservern gespeichert würden. Er gebe damit Daten beim Surfen im Internet freiwillig preis. Zudem müsse der Nutzer auch mit der Installation von „Cookies“ rechnen.

Gegenüber der Bundesregierung habe ich hingegen die Auffassung vertreten, dass es für die vom BKA betriebene Homepage-Überwachung an einer Rechtsgrundlage fehlt. Informationen darüber, wer wie oft auf eine bestimmte Website zugreift hat, sind Angaben zu den näheren Umständen der Telekommunikation, die durch Artikel 10 GG geschützt sind. Stellt ein Anbieter eine Website ins Netz, handelt es sich um ein Angebot im Bereich der Telemedien. Der Umgang mit den beim Anbieter eines solchen Angebots anfallenden Nutzungsdetails richtet sich abschließend nach dem Telemediengesetz, welches keine Befugnis für die vom BKA vorgesehene Verwendung der Nutzungsdetails einräumt (s. o. Nr. 7.9). Selbst wenn die Strafprozessordnung zur Anwendung käme, reichte § 163 StPO als Rechtsgrundlage für die heimliche Homepage-Überwachung im Hinblick auf den damit verbundenen Eingriff in das informationelle Selbstbestimmungsrecht überwiegend unbescholtener Personen nicht aus.


7.11 Kontroverse: Auskunft über Inhaber von IP-Adressen

Seit langem ist strittig, auf welcher Rechtsgrundlage ein Provider Auskunft über den Inhaber einer IP-Adresse geben muss.


Strittig ist, welche Vorschrift als Grundlage für ein Auskunftsersuchen herangezogen werden muss. Unstrittig ist, dass es sich bei den Protokolldaten um Verkehrsdaten (und nicht um Bestandsdaten) der Telekommunikation handelt (s. Kasten zu Nr. 7.8). § 113 TKG verpflichtet die Provider, den Strafverfolgungs- und Sicherheitsbehörden die Bestandsdaten eines Kunden auf Anfrage unverzüglich mitzuteilen, und es gibt dabei keine besonderen Voraussetzungen an das Auskunftsersuchen. Die Anfragen seien auf Bestandsdaten gerichtet, auch wenn zur Ermittlung der Identität der Person hinter einer IP-Adresse Verkehrsdaten hinzugezogen werden müssten, argumentieren die Befürworter dieser Rechtsgrundlage. Entsprechend hat z.B. die Bundesnetzagentur die Deutsche Telekom AG verpflichtet, Auskünfte zur Identität von Internet-Nutzern auf Basis von § 113 TKG zu erteilen. Gegen diesen Bescheid hat die Deutsche Telekom AG Widerspruch eingelegt, eine Entscheidung liegt noch nicht vor.

Weil zur Ermittlung der Person, die Telekommunikationsdienste in Anspruch genommen hat, Verkehrsdaten genutzt werden müssen, vertrete ich die Auffassung, dass die entsprechenden Bestandsdaten nur auf Grundlage des § 100g StPO an Strafverfolgungsbehörden herausgegeben werden dürfen. Dies setzt – außer in Einzelfällen – einen richterlichen Beschluss voraus. Das Gesetz sieht für die vom Fernmeldegeheimnis geschützten Verkehrsdaten eine höhere Eingriffsschwelle vor als für eine „einfache“ Bestandsdatenabfrage nach § 113 TKG.

Besonders deutlich wird die Unzulänglichkeit der Vorschrift des § 113 TKG im Zusammenhang mit Auskunftsersuchen, die Kunden von sog. Resellern der Provider betreffen. Ohne sie zu „kennen“, vergibt der Provider auch für diese Kunden die dynamischen IP-Adressen, da er seine Technik für die Reseller zur Verfügung stellt. Ohne sie zu „kennen“, vergibt der Provider auch für diese Kunden die dynamischen IP-Adressen, da er seine Technik für die Reseller zur Verfügung stellt. Anfragen der Ermittlungsbehörden werden daher an ihn gerichtet. Da er die nach § 113 TKG geforderte Auskunft zu den Bestandsdaten nicht erteilen kann, stellt sich die Frage, ob die Auskunft, welcher Reseller die Daten liefern kann, von dieser Vorschrift gedeckt ist oder ob eine erneute Anfrage nach § 161a StPO zur Zeugenaussage erfordert.

Mit Einführung der Vorratsdatenspeicherung wurden – am Ende des parlamentarischen Verfahrens und daher weitgehend unbemerkt – durch einen knappen Einschub im Gesetzentext die Vorratsdaten für Auskunftsersuchen nach § 113 TKG „geöffnet“. Damit soll nun klargestellt sein, dass IP-Adressen grundsätzlich auf dieser Rechtsgrundlage zu beauskunften sind. Diese „Klarstellung“ an unerwarteter Stelle als solche zu erkennen und zu verste-
hen, verlangt schon genaues Hintergrundwissen, vor allem hinsichtlich ihrer Entstehungsgeschichte. Das Bundesverfassungsgericht hat in seiner einstweiligen Anordnung zur Vorratsdatenspeicherung diese Nutzung leider nicht eingeschränkt.


7.12 Auf dem Prüfstand: die Telekommunikations-Richtlinien


Daten müssen während der Erhebung, Verarbeitung und Nutzung unversehrt, vollständig und ordnungsgemäß verarbeitet werden, um den verfassungsrechtlichen Vorgaben gerecht zu werden. Zudem ist eine bessere Verzahnung der Regelungen dringend geboten.


Kasten a zu Nr. 8

<table>
<thead>
<tr>
<th>Stichwort Sicherheitsziele:</th>
<th>Verwendungsberechtigung:</th>
<th>Nur Befugte dürfen Daten zur Kenntnis nehmen.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrität:</td>
<td>Verfügungsberechtigung:</td>
<td>Daten müssen während der Erhebung, Verarbeitung und Nutzung unversehrt, vollständig und ordnungsgemäß verarbeitet oder genutzt werden können.</td>
</tr>
<tr>
<td>Verfügbarkeit:</td>
<td>Authentizität:</td>
<td>Daten müssen jederzeit ihrem Ursprung zugeordnet werden können.</td>
</tr>
<tr>
<td>Authentizität:</td>
<td>Revisionsfähigkeit:</td>
<td>Es muss feststellbar sein, wer wann welche Daten in welcher Weise erhoben, verarbeitet oder genutzt hat.</td>
</tr>
<tr>
<td>Revisionsfähigkeit:</td>
<td>Transparenz:</td>
<td>Die Verfahren zur Erhebung, Verarbeitung und Nutzung müssen nachvollziehbar und ordnungsgemäß verarbeitet werden.</td>
</tr>
</tbody>
</table>


8 Technologischer Datenschutz

Immer enger sind Fragen zur Informationstechnologie oder ihres Einsatzes mit rechtlichen Fragestellungen verknüpft. Das Urteil des BVerfG zur Online-Durchsuchung vom 27. Februar 2008 setzt hier neue Maßstäbe.

8.1 Videoüberwachung

Das gemeinsam mit dem BSI entwickelte Schutzprofil für Videoüberwachungsanlagen zeigt Wirkung. Der Betrieb einer Videoüberwachungsanlage ist mit genormten Infoteichen anzudeuten.


Bei meinen Beratungen und Kontrollen von Videoüberwachungsanlagen auf Bahnhöfen und Flughäfen hat sich herausgestellt, dass die unterschiedlichsten Hinweisschilder bei der Kennzeichnung der videoüberwachten Bereiche zum Einsatz kommen. Um einen hohen Erkennungswert der Videoüberwachung zu gewährleisten, müssen genormte Hinweisschilder nach DIN 33450 (Video-Infozeichen) angebracht werden (s. Kasten zu Nr. 8.1).

Das inzwischen abgeschlossene Forschungsprojekt „Foto-Fahndung“ des BKA am Mainzer Hauptbahnhof (s. Nr. 6.3; 21. TB Nr. 5.2.6) hatte im Hinblick auf die Erkennungsgenauigkeit ein unbefriedigendes Ergebnis. Gleichwohl werde ich die Entwicklung der Videotechnologie und ihre mögliche Verknüpfung mit Ansätzen zur biometrischen Identifikation von Personen weiterhin aufmerksam beobachten. Von besonderem Interesse dürfte dabei die Weiterentwicklung datenschutzfreundlicher Verfahren sein, etwa NMO-Detektoren (Non Moving Objects) zur Erkennung z. B. herrenloser Gegenstände im Aufnahmebereich von Videoüberwachungssystemen.

Abbildung zu Nr. 8.1

**Video-Infozeichen nach DIN 33450**

Graphisches Symbol zum Hinweis auf Beobachtung mit optisch-elektronischen Einrichtungen (Video-Infozeichen) vom Deutschen Institut für Normung e. V., DIN

### 8.2 Verschlüsselung wichtig, aber immer noch nicht selbstverständlich

Eine aktuelle Umfrage bei der Bundesverwaltung zeigt, dass personenbezogene Daten beim Versand per Datenträger immer noch viel zu selten verschlüsselt werden.


Die Abfrage hat im Einzelnen folgendes Bild ergeben:

Obwohl die Vernetzung innerhalb der Bundesverwaltung sehr weit fortgeschritten ist, ist die Datenübermittlung per Datenträger bei vielen Bundesbehörden nach wie vor die Regel.


Auch besonders schutzwürdige Daten i. S. v. § 3 Absatz 9 BDSG sind betroffen, etwa Gesundheitsdaten, Daten über Straf- und Bußgeldverfahren, Personaldaten und Beihilfebeträge.

Die Übermittlung/Versendung war nur zum Teil abgesichert. So kamen nur vereinzelt Verschlüsselungsprogramme, und zwar mit sehr unterschiedlicher Qualität zum Einsatz, darunter auch völlig unbekannte Verschlüsselungsprogramme und ungeprüfte Eigenentwicklungen.

Der Versand der Datenträger ohne Schutzmechanismen stellt allerdings die überwiegende Mehrzahl dar. Insgesamt lässt sich für die Versendung von Datenträgern und die dabei eingesetzten Sicherungsmaßnahmen folgendes feststellen:

- Verschlüsselung mit Chiasmus bei ca. 10 Prozent der Abfrage,
- Verschlüsselung mit anderen Verfahren bei ca. 30 Prozent,
- keine Verschlüsselung; Postversand ohne Sicherung bei ca. 45 Prozent,
- keine Verschlüsselung; Postversand mit Sicherung z. B. Wertpaket bei ca. 5 Prozent,
- Postversand plus Passwortschutz auf dem Datenträger bei ca. 5 Prozent,
- keine Angaben bzw. ungenügende Angaben bei ca. 5 Prozent.

Maßnahmen zur Sicherung der Integrität der Daten werden in der Regel nicht vorgenommen. Digitale Signaturen werden überhaupt nicht eingesetzt. Das hat zur Folge, dass nachträgliche Änderungen der Daten nicht erkannt werden können.
werden können. Zudem beeinträchtigt dieser Mangel die Beweiskraft der übermittelten Informationen.

Bei etwa nur der Hälfte der Behörden existieren – jedoch zum Teil veraltet – Richtlinien, die den Versand von Datenträgern regeln.

Zur Frage einer Sicherungskopie der übermittelten Daten konnte ich folgendes ermitteln:

- 1/3 der Behörden speicherte eine 1:1 Kopie der übermittelten Daten.
- 1/3 der Behörden verzichtet ganz auf eine Sicherungskopie der übermittelten Daten und kann auch keine Daten rekonstruieren. In diesen Fällen würde das Abhandenkommen eines Datenträgers zu irreversiblen Datenverlusten führen.


Eine Kontrolle der Vorschriften wurde in der Regel weder durch den behördlichen Datenschutzbeauftragten noch den Sicherheitsbeauftragten oder die Innenrevision durchgeführt.

Ich habe die Umfrage zum Anlass genommen, zusammen mit dem BSI eine Empfehlung zum sicheren Datenträgerversand zu entwickeln, die auch in das IT-Grundschutzhandbuch und den Maßnahmenkatalog einfließen soll.

### 8.3 Effektive Datenlöschung

**Immer wieder werden Fälle bekannt, bei denen zum Verkauf angebotene gebrauchte Festplatten von PC nicht ausreichend sicher gelöscht werden. Oftmals sind sensible personenbezogene Daten und persönliche Fotos direkt einsehbar oder können ohne großen Aufwand rekonstruiert werden.**


Keine persönlichen Daten auf ausgerichteten PC vergessen!

Tipps zur Vermeidung einer bösen Überraschung


Aber Vorsicht, denn wenn ein System mit der CD gebootet wird, wird jede vorhandene Festplatte gelöscht!

Unter Linux/Unix sind wipe oder das universelle und im Betriebssystem integrierte Tool „dd“ zum Überschreiben mittels Zufallszahlen nutzbar.

Zu beachten ist, dass auch Memory-Sticks und Speicherkarten z. B. aus Mobiltelefonen und Digitalkameras oftmals vertrauliche Daten enthalten und sicher entsorgt oder vor der Weitergabe sicher gelöscht werden müssen. Bei diesen Speichemedien kann ggf. schon das mehrfache Überschreiben zum gewünschten Erfolg führen. Zum sicheren Löschen auf derartigen Datenträgern gibt es auch kommerzielle Lösungen, die auf den einschlägigen Internet-Seiten gelistet sind.

Beim Neukauf von Festplatten empfiehlt sich auch der Abschluss einer Option, die oft mit Keep Your Drive bezeichnet ist und es im Garantiefall ermöglicht, die defekte Festplatte zu behalten.

Also nicht vergessen: Persönliche Daten vor der Weitergabe von Festplatten und anderer Hardware unbedingt sicher und unumkehrbar löschen!

8.4 Verbesserte IT-Sicherheit – aber nicht zu Lasten des Datenschutzes!

Im Regierungsnetz des Bundes, dem Informationsverbund Berlin-Bonn (IVBB), sollen weitere Filter und Schutzmechanismen installiert und das BSI mit neuen Befugnissen ausgestattet werden, um Schadprogramme zu erkennen und zu bekämpfen. Aber nicht alles, was mehr Sicherheit bringen soll, ist auch datenschutzrechtlich hinnehmbar.


Die Angriffe auf die IT-Sicherheit beeinträchtigen nicht nur die ordnungsgemäße Abwicklung von Verwaltungsauflagen, sondern bringen Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich. Daher sind Konzepte gefragt, die sowohl den Schutz der Privatsphäre gewährleisten und zugleich die IT-Sicherheit verbessern. Sie sollten bereits beim Systementwurf greifen und nicht erst nachträglich hinzugefügt werden müssen.


Die Betreiber der „Netze des Bundes“, aber auch die Verantwortlichen für die übergreifenden Netze der Verwaltung in Europa sind aufgefordert, bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer zu berücksichtigen.
Kasten zu Nr. 8.4

Das Bundeskabinett hat Anfang 2009 den Gesetzentwurf zur Stärkung der Sicherheit in der Informationstechnik des Bundes beschlossen. Mit dem Gesetz sollen dem BSI weitere Befugnisse eingeräumt werden, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Auch wenn das mit dem Gesetzentwurf verfolgte Ziel, die IT-Sicherheit zu verbessern, grundsätzlich anzuerkennen ist, bestehen erhebliche Bedenken gegen

– die Ermächtigung des BSI, die gesamte Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung auszuwerten,

– die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden, und an den Verfassungsschutz übermittelt werden und

– den Verzicht auf die Verpflichtung des BSI, ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor zu erwartenden Angriffen (Spionage und Sabotage) zu warnen. Offenbar handelt es sich dabei um eine Konsequenz der Einführung der Online-Durchsuchung nach dem BKA-Gesetz (vgl. Nr. 4.3.1).

8.5 Kennzeichnungspflichten – Überlegungen zur Rückverfolgung von personenbezogenen Daten

Verbraucher können sich nicht wirksam gegen die ungewollte Verwendung Ihrer Daten wehren, wenn sie nicht wissen, aus welcher Quelle die Daten stammen. Unternehmen sollten dazu verpflichtet werden, die Herkunft und somit den rechtmäßigen Erwerb der Daten durch spezielle Kennzeichnung zu belegen.

Die Veräußerung von personenbezogenen Daten ist vor allem für den Handel ein zunehmend lukratives Geschäft. Unternehmen, die Kundendaten z. B. bei Bestellvorgängen vom Verbraucher erheben, geben diese oftmals gegen Entgelt, aber ohne explizite Zustimmung der Betroffenen (Opt-In) an andere Unternehmen weiter. Zudem werden Daten unrechtmäßig, also durch gezielte Angriffe von Hackern oder durch Insider entwendet. Um die zweifelsfreie Herkunft und den rechtmäßigen Erwerb von gehandelten Daten nachweisen zu können, wird darüber nachgedacht, personenbezogene Daten bereits bei ihrer Erhebung sicher zu kennzeichnen.


Auszugspunkt der Überlegungen des AK Technik war die Forderung, dass für Betroffene nachvollziehbar sein sollte, von wem die Daten erhoben wurden, auf welchem Weg ihre Daten zu Absendern von Werbepost oder anderen Kommunikationspartnern gelangen sind und wer sich dabei ggf. nicht auf die Einwilligung des Betroffenen stützen kann. Dabei können selbst technisch perfekte Verfahren lediglich der Revision dienen. Auch sie können nicht verhindern, dass bei entsprechender krimineller Energie oder bei bewusster Missachtung von Kennzeichnungspflichten Daten unberechtigt weitergegeben werden. Unabhängig von der technischen Realisierung sind zunächst verschiedene Verfahren denkbar:

– Der Ersterheber dokumentiert den Ursprung der Daten und ggf. die Einwilligung des Betroffenen in die Weitergabe. Jeder weitere Nutzer der Daten vermerkt nachwiegend, woher die Daten erworben und an wen sie weitergegeben wurden. Nachteilig ist, dass jeder auch nur kurzfristige Nutzer der Daten dauerhaft Informationen zum verwendeten Datensatz speichern muss.


– Informationen zur Herkunft und Einwilligung könnten bei einer unabhängigen und vertrauenswürdigen dritten Stelle gespeichert werden. Allerdings würde sich bei einer solchen dritten Stelle ein sehr großer Datenbestand ansammeln und auch diese könnte zudem die Herkunftskette nachvollziehen.

Es ist in jedem Einzelfall abzuwägen, ob es vertretbar ist, für die lückenlose Nachvollziehbarkeit der Herkunftskette von Daten neue Datenbestände zu erzeugen.

Es sind Speicherfristen zu definieren und ggf. elektronische Kennzeichnungsmöglichkeiten, wie die Nutzung von pseudonymen Signaturen oder andere Verfahren, zu prüfen.
In der Diskussion sind auch weitere vor allem technische Verfahren wie elektronische Signaturen, DRM (Digital Rights Management), digitale Wasserzeichen oder Sticky Policy (s. Kasten zu Nr. 8.5), welche jedoch eines gewissen Implementationszeitraums und ggf. einer Weiterentwicklung bedürfen. Sie erscheinen deshalb derzeit nicht so schnell umsetzbar:


Kasten zu Nr. 8.5

**Technische Verfahren zur Kennzeichnung von Daten**

- *Elektronische Signatur:*
  Hierzu muss jede Stelle, die Adressdaten weitergibt, die Datensätze signieren. Der Empfänger der Daten muss dann jeweils die Signaturen auf ihre Gültigkeit hin überprüfen. Trägt ein Datensatz keine Signatur, handelt es sich um ein direkt beim Betroffenen erhobenes Datum bzw. um einen Datensatz, der nicht von einem Zwischenhändler bezogen wurde. Mithilfe von elektronischen Signaturen kann der Herkunfts nachweis so anhand der aufgebauten Signaturkette nachvollzogen werden.

- *Digitales Rechtemanagement (DRM):*

- *Digitales Wasserzeichen:*
  Der Herkunfts nachweis könnte mittels eines digitalen Wasserzeichens im Adressdatensatz integriert werden. Denkbar ist auch der Einsatz so genannter „fragiler Wasserzeichen“, um Manipulationen am Datensatz erkennen zu können. Wegen des geringen Datenvolumens eines Adressdatensatzes erscheint die Unterbringung eines Wasserzeichens jedoch nur schwer möglich. Denkbar wäre jedoch die Markierung ganzer Dokumente. Um bei mehreren vorhandenen Markierungen feststellen zu können, wann welches eingebracht wurde, wäre zudem ein kryptographischer Zeitstempeldienst notwendig.

- *Sticky Policy:*
Zwecke der eindeutigen Identifizierung aller Steuerpflichtiger

Leider lag das von mir mehrfach angemahnte endgültige Einführung der Steuer-ID erläutern zu lassen.


Dies gilt auch für jede Erweiterung der beim BZSt nach § 139b Absatz 3 AO eingerichteten Datenbank (s. Nr. 9.2; 9.3) und insbesondere dann, wenn sensible Daten an das BZSt übermittelt werden sollen. Dies betrifft etwa den Melderegister der Kommunen vermerkte Übermittlungssperren, die einem besonderen Schutz unter- liegen. Melderegistersperren werden eingerichtet, wenn vom Betroffenen glaubhaft gemacht werden kann, dass eine Weitergabe der Meldedaten eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen herbeiführt. Meldebehörden dürfen die Datensätze dieser Personen nur übermitteln, wenn hierfür eine eindeutige gesetzliche Grundlage geschaffen wird. Entsprechend habe ich es begrüßt, als in der Mitteilungsschreiben des BZSt zur Steuer-ID 9.1 Identifikationsnummer für steuerliche Zwecke (Steuer-ID) – rechtlicher Rahmen – unter der Vertriebenenproblematik betroffenen Datensätze mehr versandt würden, bis bei den Meldebehörden eine Korrektur erfolgt sei. Auch werde sichergestellt, dass Betroffene, die bereits ein Mitteilungsschreiben erhalten hatten, ein korrigiertes Schreiben übersandt werde. Als weitere problematische Fälle sind anzuführen:

In Mitteilungsschreiben des BZSt wurden zum Teil sach- fremde Eintragungen wie der Name des Vermieters, der Name des ehemaligen Eigentümers sowie ein Kürzel hinsichtlich der Wohnsitzangaben des Steuerpflichtigen EFH (Einamilianenhaus) oder MFH (Mehrfamilienhaus) aufge- nommen. Das BMF teilt mir hierzu mit, dass es keine potentiell von der Vertriebenenproblematik betroffenen Datensätze mehr versandte. Dieses Vorgehen des BZSt werde ich nach § 25 BDSG als ein angemessenes IT-Sicherheitskonzept betrieben.
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen


Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Dienstanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Absatz 6 Telemediengesetz).


Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.
9.2 Was die Abgeltungssteuer mit der Religionszugehörigkeit zu tun hat

Die umfangreiche Datenbank beim Bundeszentralamt für Steuern (BZSt) wird um ein weiteres sensibles Datum, die Religionszugehörigkeit, erweitert.


Leider scheint die sich mit der Einführung der Abgeltungssteuer bietende Chance zur Verringerung des Umfangs der Verarbeitung personenbezogener Daten (vgl. 25. TB Nr. 7.3) weitgehend ungenutzt zu bleiben. Zudem befinde ich mich in Erwartung der vom BZSt eingerichteten Datenbank zur Steuer-Identifikationsnummer (vgl. Nr. 9.1) kritisch, vor allem, weil zusätzliche besonders geschützte Daten, wie die Religionszugehörigkeit, aufgenommen werden sollen (s. Nr. 9.3).


Letztlich ist zu befürchten, dass die Einführung der Abgeltungssteuer so zu einer umfangreicheren und nicht zu einer reduzierten Verarbeitung personenbezogener Daten führt.

9.3 Jahressteuergesetz 2008 – Ablösung der Lohnsteuerkarte durch ein elektronisches Abrufverfahren

Mit dem Jahressteuergesetz 2008 wurde die rechtliche Grundlage für die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren geschaffen. Hierzu wird die beim Bundeszentralamt für Steuern (BZSt) errichtete Datei um weitere sensible Daten (Lohnsteuerabzugsmerkmale) ergänzt. Von der zu- nächst vorgesehenen Einführung des schutzwürdigen „Anteilsverfahrens“ wurde abgesehen.

Das am 8. November 2007 verabschiedete Jahressteuergesetz 2008 beinhaltet einige schutzwürdiges rechtliche bedeutende Neuregelungen. Mit § 39e EStG erhöht es den Weg für die Ablösung des Lohnsteuerverfahrens mittels Lohnsteuerkarte durch ein elektronisches Abrufverfahren (ElsterLohn II) ab dem Jahre 2011. Der Arbeitgeber erhält die Lohnsteuerabzugsmerkmale, die ihm die Beurkundung der einzuhalten Gebühren und die Kirchensteuer der bei ihm beschäftigten Arbeitnehmer ermöglichen, nicht mehr durch die Lohnsteuerkarte, sondern elektronisch beim BZSt. Der Arbeitgeber (bei Beschäftigungsbeginn) erhält die Möglichkeit, die den jeweiligen Arbeitnehmer beim BZSt gespeicherten Lohnsteuerabzugsmerkmale wie Steuerklasse, Religionszugehörigkeit (auch für Ehepartner und Kinder einschließlich der Steuern (BZSt) errichtete Datei um weitere sensible Daten (Lohnsteuerabzugsmerkmale) ergänzt. Von der zu- nächst vorgesehenen Einführung des schutzwürdigen „Anteilsverfahrens“ wurde abgesehen.

Die datenschutzrechtlichen Bedenken, die von den Daten- 
tenschutzbeauftragten der Länder geteilt werden (s. Ent- 
schließung der 74. Datenschutzkonferenz, Kasten a zu Nr. 9.3), wurden im Gesetzgebungsverfahren leider nicht berücksichtigt.

Auch hinsichtlich der Sicherheit des Authentifizierungs-
verfahrens über das ELSTER-Portal bin ich nach wie vor skeptisch. Wie ich bereits im 21. TB (Nr. 4.4.1; 8.4) aus-
führliegh berichtet habe, ist zwar gemäß § 87a Absatz 3 AO die Zulassung der qualifizierten Signatur für 
Steuerpflichtige obligatorisch; daneben kann aber gemäß § 87a Absatz 6 AO unter den näheren Voraussetzungen 
der Steuerdatenübermittlungs-Verordnung (StDÜV) ein 
deres sicheres Verfahren zugelassen werden, das die 
Authentizität und die Integrität des übermittelten elektroni-
nischen Dokuments sicherstellt. Bei der Beurteilung, ob 
das ELSTER-Authentifizierungsverfahren diesen Anfor-
derungen genügt, ist zu berücksichtigen, dass sich mit der 
Entwicklung der Technik das Angriffspotential auch auf 
für Dritte „interessante“ Daten erhöhen wird und deshalb 
permanent Nachbesserungen des Authentifizierungs-
verfahrens erforderlich sein werden. Dementsprechend hat 
die 76. Datenschutzkonferenz (s. Kasten b zu Nr. 9.3) 
darauf hingewiesen, dass das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz im Hin-
blick auf die Authentizität und Integrität elektronisch 
übermittelter Dokumente derzeit maßgeblich sein müsse.

Außerdem müssten die Steuerpflichtigen die Möglichkeit 
haben, ihre elektronische Kommunikation mit der 
Finanzverwaltung durch die qualifizierte elektronische 
Signatur abzusichern.

Folgende Punkte sind datenschutzrechtlich kritisch:

# Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohneri-
nen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohn-
steuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zen-
tralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand 
würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht 
in einem Steuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Per-
sonenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitsverwägungen sind für eine Datenhaltung auf 
Vorrat in keinem Fall ausreichend.

# Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkar-
tenverfahrens durch ein elektronisches Abrufverfahren 
werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete 
Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder 
und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufge-
nommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/ Arbeitnehmerinnen sind.

Kasten a zu Nr. 9.3

Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87a Absatz 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform „Elster“ für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139b Absatz 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b Absatz 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.


Die Konferenz sieht es kritisch, dass § 150 Absatz 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Ver- einfachung des automatisierten Besteuerungsverfahren anstelle der qualifizierten elektronischen Signatur ein solches Verfahren einzuführen. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalautweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierung- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Finanzverwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronischen Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1) Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelten Dokumentes derzeit alternativlos.
2) Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.
3) Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.


Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

Mit dem Steuerbürokratieabbaugesetz (Bundesratsdrucksache 547/08) sollen u. a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Absatz 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Absatz 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Ver- einfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein solches Verfahren einzuführen. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalautweises möglich sein soll.

Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierung- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Finanzverwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronischen Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1) Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelten Dokumentes derzeit alternativlos.
2) Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.
3) Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.
9.4 Kontenabrufverfahren durch die Finanzämter und andere Behörden

Der Gesetzgeber musste die vom Bundesverfassungsgericht wegen mangelnder Bestimmtheit für verfassungswidrig erklärte Rechtsgrundlage in der Abgabenordnung neu fassen.


Mit den Datenschutzbeauftragten der Länder habe ich gefordert, die Neuordnung vor allem im Hinblick auf das verfassungsrechtliche Gebot der Normenklarheit und Transparenz zu überarbeiten (s. 20. TB Kasten b zu Nr. 8.3).


Der Gesetzgeber hat dementsprechend § 93 Absatz 8 AO neue Fassung durch insgesamt drei Absätze (§ 93 Absatz 8 bis 10 AO neue Fassung) ersetzt. Aus § 93 Absatz 8 AO ergeben sich mittelbar die Behörden, die zum Kontenabruf berechtigt sind, die Abrufvoraussetzungen und Zweckbestimmungen. So können z. B. durch die Arbeitsverwaltung Kontenabrufe im Rahmen der Überprüfung der Berechtigung zum Bezug von Arbeitslosengeld II erfolgen. § 93 Absatz 9 AO bestimmt, dass der Betroffene grundsätzlich auf die Möglichkeit des Kontenabrufs vorab hinzuweisen und über dessen Durchführung zu benachrichtigen ist, nennt aber auch Ausnahmen von dieser Hinweis- und Benachrichtigungspflicht, etwa soweit die Benachrichtigung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Er suchenden liegenden Aufgaben gefährden würde. § 93 Absatz 10 AO legt schließlich fest, dass ein Antrag auf Kontenabruf und dessen Ergebnis vom Antragsteller zu dokumentieren sind.


Besonderes kritisch sehe ich es, dass das Kontenabruffahren nicht nur für öffentlich-, sondern auch für privatrechtliche Zwecke genutzt werden sollen. So sieht etwa der Entwurf eines Gesetzes zur Reform der Sacheschließung in der Zwangsvollstreckung (Bundestagsdrucksache 16/10069) eine Auskunftsmöglichkeit des Gerichtsvollziehers zur Durchsetzung titulierter zivilrechtlicher Ansprüche vor (§ 802 Absatz 1 ZPO-E).

9.5 Auskunftsanspruch in der Abgabenordnung

Obwohl das BMF zugesagt hat, ein Auskunftsrecht analog § 19 BDSG in die Abgabenordnung aufzunehmen, ist noch immer keine gesetzliche Regelung vorhanden.


Diese richterliche Klarstellung ist auch deshalb so wichtig, weil es kaum ein anderes, für die Bürgerinnen und Bürger ähnlich bedeutendes Gebiet hoheitlichen Han delns gibt, das fast 30 Jahre nach Inkrafttreten des BDSG und 25 Jahre nach dem Volkszählungsurteil des BVerfG vergleichbar große datenschutzrechtliche Defizite aufweist wie die AO.

Das BMF machte daraufhin den Vorschlag, § 19 BDSG durch eine Bestimmung der AO „für entsprechend anwendbar“ zu erklären.


Die Mehrheit der Länder habe sich dafür ausge- sprochen, das Auskunftsrecht zunächst im Wege einer bundeseinheitlichen Verwaltungsanweisung zu regeln. Danach soll den Beteiligten auf Antrag Auskunft über die zu ihrer Person gespeicherten Daten erteilt werden, jedoch nur wenn sie ein berechtigtes Interesse darle- gen.


10 Gesundheit und Soziales

10.1 Das Gendiagnostikgesetz: Der Anfang ist gemacht

Die Arbeiten an einem Gendiagnostikgesetz kommen end- lich voran.


meine Erforschung von Ursachenfaktoren menschlicher Eigenschaften gehe, die nicht auf konkrete Maßnahmen gegenüber einzelnen Personen abziele. Das ist zwar generell zutreffend, Ziel der genetischen Forschung ist aber auch, die Wechselbeziehung zwischen genetischen und Umweltfaktoren aufzuklären und konstitutionelle Faktoren zu identifizieren, die dann zu bestimmten An- und Auffälligkeiten führen.

Wird die Forschung nicht in das GenDG einbezogen, richtet sich der Datenschutz für diesen Bereich nach den Bestimmungen des BDSG und der Ländergesetze. Dies ist nicht sinnvoll, da diese Gesetze nur allgemeine Vorgaben enthalten.

Ferner fehlen im Gesetzentwurf Regelungen für vorhandene Gendatenbanken. Pseudonymisierungsverfahren in diesen Datenbanken werden also auch in Zukunft nicht verbindlich vorgeschrieben und auch die Rechte der Betroffenen bleiben hier unklar.


Bei den nun ausstehenden parlamentarischen Beratungen werde ich mich dafür einsetzen, die genannten Regelungslücken zu schließen.

10.2 Gesetzliche Krankenversicherung
10.2.1 Steuerungsmaßnahmen der gesetzlichen Krankenkassen

Versorgungsmanagement ist erwünscht, aber ohne Druck und datenschutzkonform.


Die datenschutzrechtliche Problematik liegt darin, dass für die Rekrutierung und DMP-Teilnehmer von den Kassen Patientendaten ohne vorherige Kenntnis oder gar Einwilligung der Betroffenen an private Dienstleister übermittelt werden. Darüber hinaus werden die Versicherten mit den massiven nachhaltigen Mail- und Telefonmarketingaktionen derart bedrängt, dass die gesetzlich gewollte Freiwilligkeit stark zu bezweifeln ist.


Das Bundesgesundheitsministerium unterstützt die Datenschutzbeauftragten in ihrer Auffassung.

Ich habe die Problematik dem Spitzenverband der Krankenkassen mitgeteilt und um Unterstützung für die Umsetzung der datenschutzrechtlichen Eckpunkte gebeten. Eine Antwort steht noch aus.
Zusammenarbeit der gesetzlichen Krankenkassen mit privaten Dritten

Gesetzliche Krankenkassen bedienen sich zur Erledigung ihrer Aufgaben in verstärktem Umfang privater Unternehmen und Ärzten, teilweise unter Verstoß gegen den Datenschutz.

Von den Krankenkassen werden private Dienstleistungsunternehmen herangezogen, um z. B. Krankenhausrechnungen zu überprüfen. Private Call-Center führen im Auftrag der Kassen die Arbeit der Versicherten durch. Die Kassen verlangen von behandelnden Ärzten, ihnen dabei behilflich zu sein, chronisch kranke Versicherte zu identifizieren, die für bestimmte Behandlungsprogramme in Betracht kommen. Dabei ist vielfach zweifelhaft, ob die Kasse die jeweilige Aufgabe überhaupt einem Dritten übertragen darf und welche Datenflüsse im Rahmen der Aufgabenerledigung in Gang gesetzt werden dürfen.

Sozialversicherungsträger – und damit auch die Krankenkassen – haben ihre vom Gesetzgeber übertragenen Aufgaben grundsätzlich selbst zu erfüllen. Sie sind deshalb im Regelfall nicht befugt, ihre Aufgaben an Dritte delegiert zu geben, die dann in eigener Verantwortung wahrnehmen. Anders als privatwirtschaftliche Unternehmen darf ein Sozialversicherungsträger nur dann Aufgaben durch einen Dritten durchführen lassen, wenn das Gesetz dies ausdrücklich vorsieht. § 80 SGB X erlaubt unter engen Voraussetzungen eine sog. Datenverarbeitung im Auftrag (s. Kasten a zu Nr. 10.2.1). Diese Sonderform der Datenverarbeitung durch einen Dritten beschränkt sich aber auf manuelle, technische oder sonstige Hilfs- und Unterstützungsleistungen zur Erfüllung der Datenverarbeitungsaufgaben. Diese gesetzlich legitimierte Auftragsdatenverarbeitung ist abzugrenzen von einer Funktionsübertragung, bei der...

Kasten zu Nr. 10.2.1


Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten


- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.

- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.

- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.

- Wenn Versicherte – zu welchem Zeitpunkt auch immer – einheitlich zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

Deshalb muss im Einzelfall sorgfältig geprüft werden, ob ein Dritter überhaupt eingeschaltet werden darf. Nach § 197b SGB V können Krankenkassen ihnen obliegende Aufgaben durch Dritte wahrnehmen lassen, wenn dies wirtschaftlicher ist, es im wohlverstandenen Interesse der Versicherten liegt und deren Rechte nicht beeinträchtigt werden (s. Kasten b zu Nr. 10.2.2). Kernaufgaben der Kassen dürfen allerdings nicht Dritten in Auftrag gegeben werden. So dürfen z. B. Beratungs- und Aufklärungsleistungen der Krankenkassen über Rechte und Pflichten der Versicherten nach dem Sozialgesetzbuch, die die Kassen gegenüber ihren Versicherten erbringen müssen (§§ 11 bis 15 SGB I), nicht an Dritte vergeben werden.

Kasten a zu Nr. 10.2.2

§ 80 Abs. 5 SGB X:
Die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nichtöffentliche Stellen ist nur zulässig, wenn

1. beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder

2. die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist und die Daten zur weiteren Datenverarbeitung im Auftrag an nichtöffentliche Auftragnehmer weitergibt, verbleiben.

Hat die Kasse eine ihr obliegende Aufgabe zulässigerweise an einen Dritten übertragen, stellt sich die Frage, ob und ggf. welche Versichertendaten dazu weitergegeben werden dürfen. Sofern es sich um Angebote an die Versicherten für Patientenschulungsmaßnahmen, besondere Behandlungsprogramme etc. handelt, dürfen Versichertendaten nicht ohne Weiteres dem Dritten übermittelt werden. Hier muss zunächst die Kasse die Einwilligung ihrer Versicherten zum Datentransfer einholen (s. hierzu auch Beitrag unter Nr. 10.2.1).

Bei der Überprüfung von Krankenhausrechnungen durch private Dienstleistungsunternehmen ist der Dienstleister bei der Aufgabenübertragung an die rechtlichen Grenzen gebunden, die auch für die Krankenkasse selbst gelten (§ 284 SGB V). In manchen Fällen haben die Krankenkassen keine eigene Befugnis zur Datenerhebung, wenn es z. B. um medizinische Fragen und Beurteilungen geht. Hier muss der medizinische Dienst der Krankenkassen nach § 275 SGB V eingeschaltet werden, was dann auch für den Dienstleister gilt. Ihm stehen keine gesonderten Rechte zu.


Kasten b zu Nr. 10.2.2

§ 197b SGB V:
Krankenkassen können die ihnen obliegenden Aufgaben durch Arbeitsgemeinschaften oder durch Dritte mit deren Zustimmung wahrnehmen lassen, wenn die Aufgabenwahrnehmung durch die Arbeitsgemeinschaften oder den Dritten wirtschaftlicher ist, es im wohlverstandenen Interesse der Betroffenen liegt und Rechte der Versicherten nicht beeinträchtigt werden. Wesentliche Aufgaben zur Versorgung der Versicherten dürfen nicht in Auftrag gegeben werden …
10.2.3 Keine Extra-Daten für den Risikostrukturausgleich

Die Praxis einiger gesetzlicher Krankenkassen, im Rahmen des morbiditätsorientierten Risikostrukturausgleichs Gesundheitsdaten ihrer Versicherten zu erheben, ist datenschutzrechtlich unzulässig.

Mit der Begründung, sich um eine möglichst valide Datengrundlage zur Durchführung des Gesundheitsfonds zu bemühen, werden Diagnoseangaben bei abtreibenden Ärzten abgefragt oder die Ärzte werden gebeten, Diagnoseangaben zu koncretisieren oder durch weitere Untersuchungen aufzuzeigen. Nach § 284 Absatz 1 Satz 1 Nummer 14 SGB V ist den Krankenkassen zwar eine Erhebung von Daten erlaubt, die zur Durchführung des Risikostrukturausgleichs (RSA) erforderlich sind. Näheres über Art und Umfang der für die Durchführung des RSA erforderlichen Daten regelt die Risikostrukturausgleichsverordnung (RSAV). Diese sieht aber lediglich vor, dass für die Weiterentwicklung und Durchführung des RSA die Krankenkassen jährlich die versichertenbezogenen Diagnosen aus den Abrechnungsunterlagen für die vertragsärztlichen Leistungen erheben (§ 30 Absatz 1 Satz 1 Nr. 6 RSAV). Zur Abrechnung im Rahmen der vertragsärztlichen Versorgung ist die Übermittlung von Patientendaten zwischen Ärzten und Krankenkassen jedoch nicht vorgesehen. Auch durch die Einholung von Einwilligungen der Versicherten kann dieser gesetzliche Rahmen nicht ausgeweitet werden.

Der Gesetzgeber hat mit Blick auf das Recht auf informationelle Selbstbestimmung eine auf das erforderliche Mindestmaß beschränkte Informationsbasis bei den Krankenkassen angestrebt. Daher sind Versuche, außerhalb des gesetzlich definierten Rahmens Diagnosen zu erlangen, datenschutzrechtlich unzulässig.

Meine Rechtsauffassung wird vom Bundesversicherungsamt als Aufsichtsbehörde über die gesetzlichen Krankenkassen geteilt.

10.2.4 Schwere Verstöße von Krankenkassen bei der Vermittlung privater Zusatzversicherungen

Im Zuge von Kontrollbesuchen habe ich bei zwei gesetzlichen Krankenkassen außergewöhnlich schwere datenschutzrechtliche Verstöße bei der Vermittlung von privaten Zusatzversicherungen festgestellt und in diesem Zusammenhang u. a. auch Strafanträge gestellt.

Nach § 194 Absatz 1a SGB V dürfen gesetzliche Krankenkassen den Abschluss privater Zusatzversicherungsverträge zwischen ihren Versicherten und privaten Krankenversicherungsunternehmen vermitteln. Bei zwei gesetzlichen Krankenkassen (der IKK Weser-Ems und der IKK Hamburg) habe ich in diesem Zusammenhang u. a. unangekündigt die Voraussetzungen und Grenzen zulässiger Vermittlungsaktivitäten kontrolliert und dabei erhebliche Datenschutzverstöße festgestellt.


Ob eine solche Vorgehensweise auch bei anderen Krankenkassen praktiziert wird/wurde, habe ich auf Grund begrenzter Personalkapazitäten und anderer wichtiger Schwerpunkte in Anspruch genommen.
Aufgrund der massiven, über einen langen Zeitraum be-triebenen datenschutzrechtlichen Verstöße habe ich sowohl gegen Mitarbeiter beider gesetzlicher Krankenkassen als auch gegen Mitarbeiter des privaten Versicherungsunternehmens bei den zuständigen Staatsanwalt- schaften Strafantrag gemäß § 85a Absatz 2 SGB X wegen Vergehen nach § 85a Absatz 1 i. V. m. § 85 Absatz 2 Nummern 1, 2, 3 und 5 SGB X gestellt. In beiden Fällen dauern die Ermittlungen noch an. Angesichts der außer- gewöhnlichen Schwere der datenschutzrechtlichen Verstöße habe ich darüber hinaus den Ausschuss für Gesund- heit des Deutschen Bundestages, die Bundesministerin für Gesundheit und die für das private Versicherungsun- ternehmen zuständige Datenschutzaufsichtsbehörde in- formiert.

10.3 Gesetzliche Unfallversicherung

10.3.1 Gutachterregelung


Mit Urteil vom 5. Februar 2008 (s. Kasten a zu Nr. 10.3.1) hat das Bundessozialgericht im Wesentlichen meine seit Langem vertretene Rechtsposition (u. a. 20. TB Nr. 19.1.3) bestätigt und festgestellt, dass § 200 Absatz 2 SGB VII auch für die von den Unfallversicherungsträgern im Laufe eines gerichtlichen Verfahrens eingeholte Gutachten gilt. Damit verbietet kein datenschutzfreier Raum während eines anhängigen Gerichtsverfahrens die seitens der Berufsgenossenschaften erhobenen Bedenken gegen die Anwendung des § 200 Absatz 2 SGB VII in diesem Verfahrensstadium sind nicht durchgreifend, was ich immer hervorgehoben habe.

Kasten a zu Nr. 10.3.1

Kernsätze des Urteils des BSG vom 5. Februar 2008 – B 2 U 8/07 R – zu datenschutzrechtlich relevanten Fragen

Der Begriff des Gutachtens ist als umfassende wis- senschaftliche Bearbeitung einer im konkreten Fall relevanten fachlichen Fragestellung durch den Sach- verständigen zu definieren.

§ 200 Abs. 2 SGB VII gilt auch für von den Unfall- versicherungs trägern im Laufe eines Gerichtsverfah- rens eingeholte Gutachten.

Ein Rechtsverstoß gegen § 200 Abs. 2 SGB VII führt zu einem Beweisverwertungsverbot des einge- holten Gutachtens.

Datenschutzfreundlich ist auch die Feststellung des Bundessozialgerichts, bei einem Verstoß gegen § 200 Absatz 2 2. Halbsatz SGB VII i. V. m. § 76 Absatz 2 SGB X bestehe grundsätzlich ein Verwertungsver-
in welchen Fällen ein Unfallversicherungsträger einen Beratungsarzt mit dem Gutachten beauftragt oder einen externen Gutachter.


Kasten b zu Nr. 10.3.1.


10.3.2 Einschränkung des Auskunftsverlangens bei Krankenkassen nach § 188 Satz 2 SGB VII

Wird die Einschränkung des Auskunftsverlangens nach § 188 Satz 2 SGB VII nicht beachtet, werden die gesetzlich festgelegten Verantwortungsregelungen verschoben.


Ich werde weiterhin auf die korrekte Gesetzesanwendung bei der Erhebung der Vorerkrankungsdaten durch die Unfallversicherungsträger hinwirken.

10.4 Gesetzliche Rentenversicherung

Der ärztliche Entlassungsbericht in der medizinischen Rehabilitation – wer darf ihn bekommen?

Der Reha-Entlassungsbericht der Deutschen Rentenversicherung ist ein ärztlicher Brief mit besonderer Bedeutung. Aber nicht jeder, der ein Interesse daran hat, darf ihn erhalten. (s. Kasten zu Nr. 10.4)

Kasten zu Nr. 10.4

**Der Reha-Entlassungsbericht**

- Er dient der Dokumentation und Information über den Behandlungsanlass bei den Rehabilitanden, den Prozessverlauf der Rehabilitation und das Rehabilitationsergebnis.

- Er umfasst darüber hinaus eine sozialmedizinische Beurteilung des Arztes der Reha-Einrichtung mit einer Aussage über die Leistungsfähigkeit des Rehabilitanden im Erwerbsleben.

- Er ist daher für verschiedene Stellen von Interesse, z. B. für den ambulant behandelnden Arzt, für den Rententräger, die Krankenkasse oder den Medizinschen Dienst der Krankenkassen als Entscheidungsgrundlage z. B. für die Zahlung von Krankengeld.


Wiederholt war klärungsbedürftig, ob die DRV Bund regelmäßig den vollständigen Reha-Entlassungsbericht erhalten darf. Nachdem die DRV Bund nachvollziehbar darlegen konnte, dass sie die Kenntnisnahme des vollständigen Berichts für die Erfüllung ihrer gesetzlichen Aufgaben benötigt, ist dies unter folgenden Bedingungen vertretbar: Es muss zum Einen sichergestellt sein, dass bereits in den Reha-Kliniken nur die erforderlichen Daten erhoben wurden. Darüber hinaus ist sicherzustellen, dass die Zugriffsmöglichkeiten auf den Entlassungsbericht innerhalb der DRV Bund datenschutzgerecht ausgestaltet werden, der Zugriff einzelner Mitarbeiter also nur erfolgt, soweit dies jeweils erforderlich ist.

10.5 Arbeitsverwaltung

10.5.1 Die Jobbörse der Bundesagentur für Arbeit in der Kritik

Verschiedene technische Maßnahmen sollen den Schutz der Teilnehmerinnen und Teilnehmer der Jobbörse gewährleisten (vgl. hierzu Nr. 7.5). In der Praxis zeigten sich aber trotzdem Probleme.


In einem anderen Fall beschwerzte sich eine Petentin darüber, dass ihre Bewerberdaten in der Jobbörse ohne ihr Wissen und Einverständnis an ebenfalls in der Jobbörse registrierte potenzielle Arbeitgeber weitergegeben worden waren. Die Petentin war Leistungsempfängerin und hatte ihre Bewerberdaten in anonymisierter Form in die Jobbörse eingestellt. Bei jeder Einstellung in der selbst verwalteten Jobbörse muss jedoch gelten, dass Daten nur mit vorherigem Einverständnis der Betroffenen einseitig an Arbeitgeber übermittelt werden dürfen, ohne Unterscheidung zwischen Leistungsempfängern und Nicht-Leistungsempfängern. Sonst könnte praktisch jeder, der sich als Arbeitgeber registrieren lässt, ohne Weiteres an die Daten anonymer Bewerber kommen. In diesem Fall hatte zur Anbahnung eines Beschäftigungsverhältnisses ein förmlicher Vermittlungsvorschlag erstellt werden müssen, sowohl der Arbeitgeber als auch die Bewerberin hätten also schriftlich informiert werden müssen. Dies wäre von der Petentin als Leistungsbezieherin auch hin-
10.5.2 Erhebung des Migrationshintergrunds von Arbeitsuchenden geplant

Die zur Verbesserung der beruflichen Eingliederung geplante Erhebung des Migrationshintergrunds im Bereich der Arbeitsverwaltung bedarf einer datenschutzkonformen gesetzlichen Regelung.


In Anlehnung an das Konzept des Mikrozensus von 2005 liegt ein Migrationshintergrund vor, wenn

- die Person nicht auf dem Gebiet der heutigen Bundesrepublik geboren wurde und 1950 oder später zugewandert ist oder
- die Person keine deutsche Staatsangehörigkeit besitzt oder eingebürgert wurde oder die deutsche Staatsbürgerschaft nach § 7 Staatsangehörigkeitsgesetz gesetzlich erworben hat,
- ein Elternteil der Person mindestens eine der unter Nummer 1 oder 2 genannten Bedingungen erfüllt.

Mit Blick auf die Bedeutung der Integration von Menschen mit Migrationshintergrund kann die Nutzung dieser Daten für die Planung von Arbeitsförderungsmaßnahmen durchaus sinnvoll sein. Allerdings ist vor der Einführung einer Registrierungspflicht des Migrationshintergrunds plausibel darzulegen, wie die Datenerhebung zu dem angestrebten Ziel beitragen soll. Aus datenschutzrechtlicher Sicht kommt es darauf an, hier keine „Migrantenetablisments“ zu schaffen, auf die am Ende jeder Vermittler zurückgreift.


Die Überlegungen im BMAS und in der Arbeitsverwaltung sind noch nicht abgeschlossen. Ich werde die entsprechenden Planungen weiterhin konstruktiv begleiten.

10.5.3 Noch kein neuer Sachstand bei der datenschutzrechtlichen Aufsicht für die Arbeitsgemeinschaften (ARGE)

Die vom Bundesverwaltungsgericht für verfassungswidrig erklärte Mischverwaltung muss bis zum 31. Dezember 2010 neu geregelt werden.


Ich habe mit den Landesbeauftragten für den Datenschutz einverstanden, dass für diese Übergangszeit im Interesse einer wirksamen datenschutzrechtlichen
Aufsichtsständigkeit die bisherige Kontrollpraxis beibehalten wird.


Die Länder haben sich gegen das vom BMAS erarbeitete Konzept ausgesprochen, insbesondere weil ausreichende Mitgestaltungsrechte der Länder fehlten. Mehrheitlich wird eine Regelung befürwortet, die eine weitgehende Selbständigkeit der ZAG als verfassungsrechtlich abgesicherte Form der Mischverwaltung ermöglicht.


10.5.4 Einzelfälle

— Weitergabe von Gesundheitsdaten an potentielle Arbeitgeber durch die Agentur für Arbeit ohne Wissen und Beteiligung der Kundin.


Hierin liegt ein schwerwiegender Datenschutzverstoß, da es sich bei Gesundheitsdaten um besonders schutzwürdige Daten handelt. Auf die Beschwerde der Petentin hin räumte die Agentur für Arbeit ein, dass zunächst der betroffene Arbeitslose darüber zu informieren ist, bevor dem jeweiligen Arbeitgeber gegenüber die Schwerbehinderung als mögliche Fördervoraussetzung mitgeteilt wird.


Ein Petent beschwerte sich darüber, dass nach einer Untersuchung durch den Ärztlichen Dienst der Agentur für Arbeit neben seinem Leistungsbild auch seine ärztlichen Befunde für seinen Vermittlungssachbearbeiter frei zugänglich waren.


Von einer förmlichen Beanstandung habe ich im vorliegenden Fall abgesehen, weil die BA meine Rechts­ausfassung teilte und die Agentur für Arbeit angewiesen hat, eine Löschung der entsprechenden Gesundheitsdaten des Petenten im Vermittlungsbereich vorzunehmen.
11 Mitarbeiterdatenschutz

11.1 Dringender Handlungsbedarf beim Arbeitnehmerdatenschutz


11.2 Angehörige erhalten ein eigenes Antragsrecht bei der Beihilfe

Änderungen im Beihilferecht des Bundes führen endlich zu mehr Datenschutz für Familienangehörige der Berechtigten.


Bereits in mehreren Tätigkeitsberichten (vgl. zuletzt 18. TB Nr. 18.5.2) hatte ich die damalige Rechtslage kritisiert, nach der allein beihilfeberechtigten Beamten selbst ein Antragsrecht zustünde.


Ich werde die Entwicklung weiter beobachten und die Fälle prüfen, in denen Familienangehörige eigene Antragsberechtigungen verlangt haben. Sollte sich herausstellen, dass die neue Regelung nicht greift, werde ich mich für eine weitergehende Änderung einsetzen.

11.3 Bewerbungsunterlagen sind nach zwei Monaten zurückzugeben oder zu vernichten

Firmen und Behörden dürfen Bewerbungsunterlagen nicht länger als unbedingt nötig behalten. Das Allgemeine Gleichbehandlungsrecht (AGG) legt hierfür eine Maximalfrist von zwei Monaten fest.


11.4 Nicht alle Aufgaben eignen sich für Telearbeit


Jedoch gibt es auch bei besonders schutzwürdigen personenbezogenen Daten Unterschiede. So können z. B. im Personaladatsystem Aus- und Fortbildungsdaten oder solche über einzelne Verwendungen durchaus geeignet sein, im Rahmen von Telearbeit verarbeitet zu werden, obgleich es sich auch dabei um Personaladaten und damit um besonders schutzwürdige personenbezogene Daten handelt. Daten über Beurteilungen oder Erkrankungen eignen sich dagegen zur häuslichen Verarbeitung nicht.
Hier wäre das unvermeidbare Restrisiko kaum hinnehmbar. Bei der Bewertung spielt auch eine Rolle, wie hoch das Missbrauchsrisiko bezogen auf die Arbeitsabläufe konkret ist. So ist die voll elektronische Datenverarbeitung ohne Medienbruch anders zu beurteilen als konventionelle Bearbeitung, bei der Akten vom Dienstbüro zum Telearbeitsplatz transportiert, dort bearbeitet und wieder zurück ins Büro geschafft werden. Daher ist in jedem Einzelfall sorgfältig zu prüfen, ob eine Verarbeitung von personenbezogenen Daten in Telearbeit datenschutzrechtlich vertretbar ist.

12 Verkehr
12.1 Verwendung der Mautdaten zur Strafverfolgung?

Auch in diesem Berichtszeitraum hatte ich mich mit der Verwendung von Mautdaten zu beschäftigen.

In meinem letzten Bericht hatte ich über die Absicht der Bundesregierung informiert, durch eine Änderung des Autobahnmautgesetzes (ABMG) die Mautdaten auch zur Verbrechensbekämpfung zu nutzen (21. TB Nr. 12.1). Die Beratungen eines seinerzeit vom BMI vorgelegten Referentenentwurfs sind letztlich ergebnislos verlaufen. Ich gehe davon aus, dass sich bei der Bundesregierung die Einsicht durchgesetzt hat, dass die vorhandenen Mautdaten entweder gar nicht oder nur sehr eingeschränkt für Strafverfolgungszwecke oder zur Gefahrenabwehr geeignet sind und sich deshalb eine Gesetzesänderung erübrigt hat.


12.2 Neues Maritimes Sicherheitszentrum soll Zusammenarbeit verbessern

Die im Zuge der Einrichtung eines Maritimen Sicherheitsszentrums in Cuxhaven vorgesehene Weitergabe von Schiffssverkehrsdaten begegnet keinen datenschutzrechtlichen Bedenken.


Ich habe besonderen Wert darauf gelegt, dass die jeweiligen Daten von den verschiedenen Behörden nur für die Zwecke genutzt werden, zu denen sie erhoben wurden; eine Zweckänderung ist nur in gesetzlich vorgegebenen Fällen zulässig. Im Rahmen ihrer gesetzlichen Aufgaben-erfüllung sind bestimmte Daten allen Behörden jederzeit verfügbar; darüber hinaus soll eine Datenübermittlung nur zulässig sein im Falle eines polizeilichen, zoll- oder fischereirechtlichen Anfangsverdachts. Auf Basis dieses Konzepts können Schiffsdaten (Name des Schiffes, Reede, Position und Geschwindigkeit) übermittelt werden. Das BMVBS hat zugesagt, ein Datenschutz- und Informationssicherheitssystem für das MSZ zu erstellen, in dem die Datenflüsse im GLZ-See in den bestimmten Eignisfällen dargestellt werden.


12.3 Online-Anbindung der örtlichen Fahrerlaubnisbehörden an das Zentrale Fahrerlaubnisregister des Kraftfahrt-Bundesamtes

Der mit der Einführung der Kartenführerscheine verbundene Aufbau des Zentralen Fahrerlaubnisregisters führte zu gesetzgeberischem Änderungsbedarf.

Seit Jahren (zuletzt 21. TB Nr. 12.5) berichte ich über die datenschutzrechtlichen Probleme bei der Online-Anbindung der örtlichen Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt (KBA). Das KBA führt das Zentrale

Nach § 51 StVG haben die FEB dem KBA unverzüglich die zu speichernden oder zu einer Änderung oder Lösung einer Eintragung führenden Daten mitzuteilen. Dabei wird offen gelassen, in welcher Weise diese Mitteilungen zu erfolgen haben. Eine „Mitteilung“ nach § 51 StVG hat zur Folge, dass das KBA diese Informationen selbst zu verarbeiten hat, somit auch für die Richtigkeit der im ZFER eingestellten Daten in vollem Umfang selbst verantwortlich ist. Tatsächlich ist es, wie ich anhand eines Besuches beim KBA festgestellt habe, aber so, dass die FEB im Wege des File Transfers (rd. 88 Prozent der Zugriffe) oder Online-Dialog-Verfahrens (rd. 12 Prozent der Zugriffe) direkt auf den Datenbestand des ZFER zugreifen, wobei das KBA jeden Zugriff protokolliert.


13 Europa und Internationales

13.1 Europäische Rechtsentwicklung


Zudem sieht der Lissabon-Vertrag in Artikel 6 Absatz 2 den Beitritt der Union zur Europäischen Menschenrechtskonvention vor, wodurch die bisherige Geltung der Gemeinschaftsgrundrechte als allgemeine Rechtsgrundsätze bestätigt würde.


13.2 Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie

Die Datenschutzgruppe hat weitere wegwiesende Papiere zum Datenschutz verabschiedet.


Breiten Raum in den Diskussionen der Gruppe nahm die Erfassung und Übermittlung von Passagierdaten ein. Im Jahre 2007 wurde das dritte Abkommen zwischen der EU und den USA geschlossen (s. u. Nr. 13.5.2). Im Sommer 2008 wurde zudem ein PNR-Abkommen mit

Fortgesetzt wurden die Arbeiten im Bereich verbindlicher Unternehmensregelungen zur Übermittlung personenbezogener Daten in Länder ohne angemessenes Datenschutzniveau (BCR-Binding Corporate Rules) (s. u. Nr. 13.2.3).


Kasten zu Nr. 13.2

Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie

Nach Artikel 29 der EG-Datenschutzrichtlinie 95/46/EG berät die Gruppe, die sich aus den nationalen Datenschutzbeauftragten zusammensetzt, die Europäische Kommission und prüft unter anderem die Umsetzung der Richtlinie in nationales Recht im Sinne einer einheitlichen Rechtsanwendung. Sie nimmt Stellung zum Schutzniveau sowohl in der Gemeinschaft als auch in Drittländern, erstellt Arbeitspapiere, um auf besondere datenschutzrechtliche Probleme aufmerksam zu machen und entwickelt Empfehlungen zum Schutze der Privatsphäre der Bürgerinnen und Bürger der Gemeinschaft.

13.2.1 Gemeinsame Aktivitäten: Europaweite Datenschutzprüfung im Krankenversicherungssektor

Nach Abschluss der Überprüfung im Krankenversicherungssektor wenden sich die europäischen Datenschutzbehörden dem Telekommunikationssektor zu.


Wegen der zunehmenden Bedeutung international agierender Unternehmen sind weitere gemeinsame Überprüfungen der europäischen Datenschutzbehörden geplant. Als nächstes werden sie sich den Internet-Providern und Telekommunikationsunternehmen zuwenden. Auf der Basis eines an die Unternehmen übersandten Fragekatalogs sollen ab Frühjahr 2009 Gespräche mit den Firmen sowie gezielte Überprüfungen stattfinden.

13.2.2 Safe Harbor

Die auf dem Safe-Harbor-Seminar im Oktober 2008 vorgestellte EU-Studie beleuchtet Vor- und Nachteile dieses Abkommens.


Angesichts der Globalisierung der Datensphäre soll der transatlantische Datenschutzdialog auf andere, den Schutz der Privatsphäre betreffende Themen, ausgedehnt werden, zum Beispiel den Konsumentenschutz und die Einhaltung datenschutzrechtlicher Standards bei sozialen Netzwerken.

13.2.3 Binding Corporate Rules

Die Artikel-29-Gruppe verstärkte ihre Anstrengungen im Bereich der verbindlichen unternehmensinternen Datenschutzregelungen (Binding Corporate Rules, BCR), die ein wichtiges Instrument für die Datenübermittlung in Drittstaaten darstellen.


Ich unterstütze diese Bemühungen.

### 13.2.4 Stellungnahme zu personenbezogenen Daten

*Die Artikel-29-Gruppe beschäftigte sich mit der Frage, wann Daten als personenbezogen anzusehen sind. Dies ist deshalb von zentraler Bedeutung, weil das Datenschutzrecht nur für personenbezogene Daten gilt.*


**Kasten zu Nr. 13.2.4**

### Der Begriff der „personenbezogenen Daten“ in der Richtlinie 95/46/EG

Die Richtlinie 95/46/EG definiert in Artikel 2 lit. a den Begriff der „personenbezogenen Daten“ weit und versteht hierunter „alle Informationen über eine bestimmte oder bestimmbare natürliche Person“. Die Artikel-29-Gruppe konzentriert sich in ihrer Analyse auf die vier Hauptbausteine der Definition und untermauert diese durch Beispiele aus der Anwendungspraxis europäischer Datenschutzbehörden. Im Folgenden sollen die zentralen Auslegungskriterien dieser Definition erläutert werden:

- **„alle Informationen“**: Einbezogen sind Informationen unabhängig von ihrer Art, Inhalt und Form. Es gibt insbesondere keineangelosten oder freien Daten, welche grundsätzlich nicht unter das Datenschutzrecht fallen.
- **„über“**: Die Informationen müssen sich in irgendeimer Form auf die Person beziehen lassen. Der Bezug kann über den Inhalt (Informationen werden über eine bestimmte Person gegeben), über den Verwendungszweck (Daten werden verwendet, um eine Person zu beurteilen, in einer bestimmten Weise zu behandeln oder ihre Stellung oder ihr Verhalten zu beeinflussen) oder über das Ergebnis der Verarbeitung (die Verwendung der Daten hat Auswirkungen auf die Person) hergestellt werden.
- **„bestimmte oder bestimmbare“**: Neben einem direkten Personenbezug ist es auch möglich, dass sich Daten indirekt auf Personen beziehen lassen. Selbst wenn der verantwortlichen Stelle die Identität einer Person nicht bekannt ist, kann es sich also um personenbezogene Daten handeln, insbesondere wenn Dritte die Informationen zu einer Person beziehen können. Zweifelsfälle entstehen insbesondere bei der Verwendung pseudonymisierter Daten. Entscheidend ist, dass die Daten bei realistischer Betrachtung unter Einbeziehung des Aufwandes und des Interesses der Person zugeordnet werden können.
- **„natürliche Personen“**: Im Sinne der europäischen Datenschutzrichtlinie ist ein Personenbezug nur bei natürlichen Personen (Menschen) möglich; juristische Personen (Körperschaften, z. B. Vereine, Aktiengesellschaften, öffentliche Stellen) werden nicht einbezogen. Ebenso wenig umfasst sind Daten über verstorbene Personen oder ungeborene Kinder.
Vor diesem Hintergrund wurde insbesondere im Zusammenhang mit der Neufassung der Datenschutzrichtlinie für elektronische Kommunikationsdienste (E-P médiCARD Directive, vgl. Nr. 7.12) intensiv darüber diskutiert, inwieweit IP-Adressen personenbezogen sind.


13.3 Europaweite Zusammenarbeit von Polizei- und Sicherheitsbehörden und von Datenschutzkontrollbehörden

Die Zusammenarbeit der Sicherheitsbehörden in der Europäischen Union gemäß dem Haager Programm wird fortgesetzt und intensiviert. Leider wird der europaweite Datenschutz in diesem Bereich nicht gleichermaßen ausgebaut.


Die verstärkte polizeiliche Zusammenarbeit in Europa macht darüber hinaus eine enge datenschutzrechtliche Kooperation der europäischen Datenschutzkontrollinstanzen, in Ergänzung der Artikel-29-Gruppe (s. o. Nr. 13.2) erforderlich. Voraussetzung für die Einsetzung eines entsprechenden Gremiums ist allerdings eine politische Entscheidung des Rates.

Rechtsakte

- „Schwedische Initiative“ (Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der EU), s. u. Nr. 13.3.6,
- Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), s. u. Nr. 13.3.4,
- Beschluss 2008/615/JI des Rates vom 20. Juni 2008 über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration, s. u. Nr. 13.3.2,
- Beschluss des Rates zur Errichtung des Europäischen Polizeiamtes (EUROPOL), s. u. Nr. 13.3.3.

Das Haager Programm von 2004 umfasst einen Zeitraum von fünf Jahren, also bis 2009. So hat im Juni 2008 eine hochrangige Gruppe, die sog. Future Group, die noch unter deutscher EU-Präsidentschaft im Jahr 2007 eingerichtet worden war, einen Bericht unter dem Titel „Freiheit, Sicherheit, Privatheit“ vorgelegt, der als Ausgangsbasis für ein Nachfolgeprogramm zum Haager Programm die-
nen könnte. Dort werden alle Aspekte der künftigen europäischen Innenpolitik abgehandelt, für die in Zukunft das Konvergenzprinzip als Leitmaxime gelten soll; dem Datenschutz (privacy) sind allerdings nur zwei von 122 Kapiteln vorbehalten, welche zudem die datenschutzrechtlichen Anforderungen nur unzureichend beschreiben. Der Bericht soll als das sog. Stockholmer Programm unter schwedischem Vorsitz verabschiedet werden. Es bedarf also noch datenschutzrechtlicher Überzeugungsarbeit, um einen verstärkten Schutz der Bürgerrechte auch unter dem Nachfolgeprogramm zu gewährleisten.

13.3.1 Rahmenbeschluss über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen


Der Rahmenbeschluss gilt zudem nicht für die Verarbeitung von Daten in Akten, in denen jedoch weiterhin ein großer Anteil der polizeilichen Datenverarbeitung stattfindet.


13.3.2 Vertrag von Prüm und dessen Überführung in europäisches Recht


Die Gesichtspunkte, die aus datenschutzrechtlicher Sicht beim ursprünglichen Vertrag von Prüm vorgebracht wurden, müssen erst recht bei der Überführung des Vertrages in europäisches Recht berücksichtigt werden, denn hier wird langfristig die DNA- und daktyloskopische Praxis aus 27 EU-Mitgliedstaaten zusammengeführt.

Wegen der dargestellten Probleme ist eine intensive grenzüberschreitende Kooperation der in den Vertragstexten ausdrücklich erwähnten nationalen Datenschutzkonzollinstanzen unerlässlich.

**13.3.3 EUROPOL**

EUROPOL erhält eine neue Rechtsgrundlage in Form eines Ratsbeschlusses. Darüber hinaus werden seine Aufgaben und Befugnisse erweitert. Diese Gelegenheit wurde nicht genutzt, um die bestehenden datenschutzrechtlichen Defizite zu beheben.

Die EU-Kommission hat am 20. Dezember 2006 den Vorschlag für einen Beschluss des Rates zur Errichtung

Die Bedeutung von EUROPOL wird auch deshalb zunehmen, weil es Zugriff auf europaweite Datenbanken wie das SIS II (Nr. 13.3.4) und das VIS (Nr. 13.3.5) erhalten soll. Die Behörde entwickelt sich auf diese Art zu einer zentralen Informationssammelstelle im Bereich der Dritten Säule der EU, was durch ihre ausdrückliche Benennung in Artikel 88 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) (vgl. Vertrag von Lissabon, s. o. Nr. 13.1) unterstrichen wird.


Mit dem Ratsbeschluss werden die Aufgaben und Befugnisse von EUROPOL erweitert. Angemessene Verbesse rungen der datenschutzrechtlichen Regelungen sind aber nur bedingt erreicht worden.


Ich gehe davon aus, dass die Verantwortlichkeit für die Feststellung der EUROPOL-Relevanz einer polizeilichen Erkenntnis nunmehr klargestellt ist und künftig nur solche Datensätze an EUROPOL übermittelt werden, die für dessen Aufgabenerfüllung erforderlich sind.

13.3.4 Schengen


Das Schengener Informationssystem (SIS)  

Durch die Erweiterung des Schengen-Raumes um die nordeuropäischen Länder Dänemark, Finnland, Schweden, Norwegen und Island und dem damit einhergehenden erhöhten Datenvolumen im SIS waren technische Anpassungen erforderlich, die mit der Inbetriebnahme des SIS I+ Anfang 2000 realisiert wurden.

Um den zum 1. Mai 2004 der EU beigetretenen Mitgliedstaaten die Teilnahme am SIS zu ermöglichen, aber auch, um das System an die wachsenden Anforderungen bei der Bekämpfung der grenzüberschreitenden Kriminalität, des internationalen Terrorismus und der illegalen Zuwanderung anzupassen, wurde im Jahr 2001 das SIS II-Projekt begonnen. Das SIS II soll neue Funktionalitäten enthalten, die u. a. Abfragen nach biometrischen Daten, wie Fingerabdrücke und Lichtbilder, ermöglichen.

Da eine Inbetriebnahme des SIS II wegen technischer und logistischer Probleme zum vorgesehenen Einführungstermin nicht möglich war, wurde als Zwischenlösung eine erweiterte Version des SIS I+ zur Verfügung gestellt. Die SISone4all, parallel zum SIS II entwickelt und im Sommer 2007 in Betrieb genommen. Damit konnten die neuen EU-Mitgliedstaaten am Schengener Fahndungsverband als Voraussetzungen für den Wegfall der Binnengrenzkontrollen teilhaben. Das SIS II soll, sobald es betriebsbereit ist, das SISone4all ersetzen.

Mit der Inbetriebnahme des neuen SIS wird die datenschutzrechtliche Kontrolle für die technische Unterstützungseinheit und die SIS II-Datenbank in Straßburg auf den Europäischen Datenschutzbeauftragten übergehen, während die Kontrolle des nationalen Systems in Deutschland, des N. SIS II, mir als für das BKA zuständige Kontrollinstanz obliegen wird. Ab diesem Zeitpunkt werden auch die Regelungen der Artikel 92 bis 119 SDÜ, die u. a. die Abfragen nach biometrischen Daten, wie Lichtbilder und Fingerabdrücke, eine umfassende Vorabkontrolle der dadurch für den nationalen Teil des SIS II entstehenden Folgen vom BMI bzw. BKA gefordert.


Der von der Bundesregierung im September 2008 beschlossene Gesetzentwurf zum Schengener Informationssystem der zweiten Generation (SIS II) war bis Redaktionsschluss noch nicht vom Bundestag verabschiedet. Er enthält im Wesentlichen die notwendige Anpassung innerstaatlicher Vorschriften als Konsequenz der o. g. europäischen Rechtsakte zur Einrichtung des SIS II. Bei der Vorbereitung des Gesetzentwurfes habe ich darauf geprüft, dass die fortlaufende Duplizierung eines Teils des Schengener Fahndungsbestandes für Zwecke der Ausländerregister und -sachen in INPOL sowie im SIS eingeräumt wurde. Dieses Gesetz ist vom BMI in diesem Schritt leider nicht aufgegriffen.

Der Entwurf des SIS-II-Gesetzes enthielt auch eine Anpassung des § 17 Absatz 3 BVerfSchG, eingeführt durch das Terrorismusbekämpfungsgesetz vom 5. Januar 2007 (BGBl. I 2007 S. 2), mit dem den Nachrichtendiensten derzeit die Rücksprache von Personen und Sachen in INPOL sowie im SIS eingeräumt wurde (21. TB Nr. 5.1.2). Da diese Regelung erstmalig die Befugnis zur Ausschreibung von Personen und Sachen in INPOL sowie im SIS eingeräumt wurde, wäre der Entwurf des SIS-II-Gesetzes weiterer Daten, u. a. weiterer biometrischer Daten (s. o.), zu einem Kernelement der Sicherheitstechnik der 25 angeschlossenen Vertragsparteien werden. Damit besteht die Gefahr, dass es sich zu einem zentralen polizei-

13.3.5 Zugriff der Sicherheitsbehörden auf das Visa-Informationssystem


Nach dem VIS-Zugangsbeschluss soll der Zugriff auf das VIS (s. auch unter Nr. 16.2) nur über zentrale Zugangsstellen in den EU-Mitgliedstaaten erfolgen. Sie prüfen, ob der Zugriff der Sicherheitsbehörden auf das VIS im Einzelfall zur Verhütung, Aufdeckung oder Ermittlung von terroristischen und sonstigen schwerwiegenden Straftaten erforderlich ist. Damit ist ein wesentliches Element des Vorschlags der Kommission (21. TB Nr. 3.2.7), die damit routinemäßige Abfragen der Sicherheitsbehörden der ursprünglich zu administrativen Zwecken erhobene Daten verhindern wollte, erhalten geblieben.


13.3.6 Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten


Durch den Rahmenbeschluss sollen die Strafverfolgungsbehörden rechtzeitig Zugang zu Erkenntnissen der Strafverfolgungsbehörden in den anderen EU-Mitgliedstaaten erhalten, um Straftaten und andere kriminelle Aktivitäten zu verhindern und zu verfolgen. Die zentrale Regelung des Rahmenbeschlusses sieht vor, für den Austausch von Informationen und Erkenntnissen mit den Strafverfol-


### Kasten zu Nr. 13.3.6

**Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6./7. November 2008**

**Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten**


Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative“ verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln,
- eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,
- Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,
- Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,
- normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,
- vollständige Umsetzung der Datenschutzbestimmungen in Artikel 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,
- normenklare Bestimmung welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,
- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.
13.3.7 Kontrolle der EU-Außengrenzen


Die Kommission hat am 13. Februar 2008 eine Mitteilung an das Europäische Parlament, den Rat und weitere Empfänger veröffentlicht, mit der sie drei Maßnahmen für ein wirksameres Border Management ankündigt:

- Vorbereitung der nächsten Schritte für die Grenzwartung in der EU,
- Prüfung der Schaffung eines Europäischen Grenzkontrollsystems (EUROSUR) und
- Bericht über die Evaluator und künftige Entwicklung der Agentur FRONTEX.


13.3.8 Tätigkeit der Datenschutzkontrollgremien

Die zunehmende polizeiliche und justizielle Zusammenarbeit zwischen den Mitgliedstaaten der Europäischen Union bedingt auch eine verstärkte grenzüberschreitende datenschutzrechtliche Kooperation.

Die zunehmende grenzüberschreitende polizeiliche und justizielle Zusammenarbeit der zuständigen Sicherheitsbehörden in den EU-Mitgliedstaaten, verbunden mit einem vermehrten Austausch personenbezogener Daten, macht zum Schutz der Bürgerrechte eine bessere grenzüberschreitende Datenschutzkontrolle erforderlich (s. auch Nr. 13.3.7). Bei der Kontrolle der EU-weit betriebenen Datenbanksysteme (SIS I+, EUROPOL-Informationssystem, Zollinformationssystem ZIS) wird dies bereits durch die gemeinsamen Datenschutzkontrollinstitute (EDPS), u. a. bei Eurodac (vgl. 21. TB Nr. 3.2.8), in Kooperation mit den nationalen Kontrollbehörden. Anzuvertrauen ist eine umfassende Datenschutzkontrolle dieser Datenbanken, die durch Kontrollen auf nationaler Ebene komplettiert wird. Die Kontrollen erfolgen sowohl vor Ort durch gemeinsame Prüfteams, z. B. bei EUROPOL (vgl. 21. TB Nr. 3.2.3.2), als auch koordiniert durch die Kontrollinstitute mittels umfangreicher Fragebögen (vgl. 21. TB Nr. 3.2.4.2 und Nr. 3.2.5). Auch beim Informationsaustausch zur Durchführung des Vertrages von Prüm haben die nationalen Datenschutzbehörden eine intensive grenzüberschreitende Datenschutzkontrolle verknüpft. Die gemeinsame datenschutzrechtliche Kontrolle muss weiter zunehmen, wenn der Vertrag von Prüm in den EU-Rechtsrahmen überführt und von 27 Mitgliedstaaten vollzogen wird (vgl. Nr. 13.3.2). Nach Inkrafttreten des Vertrages von Lissabon (vgl. Nr. 13.1) dürften die meisten der europaweit oder durch europäische Institutionen betriebenen Datenbanken der datenschutzrechtlichen Kontrolle durch den EDPS unterfallen, der zur Durchsetzung eines gleichwertig hohen Datenschutzniveaus auf die Zusammenarbeit mit den nationalen Datenschutzkontrollinstituten angewiesen sein wird.

Die nachgeordnete Datenschutzkontrolle bedarf der Ergänzung durch proaktive Maßnahmen. Datenschutz muss also bereits bei der Entscheidung über die einschlägigen europäischen Rechtsakte und bei der Einrichtung entsprechender Datenbanken berücksichtigt werden. Es bedarf eines Forums der unabhängigen Datenschutzbehörden aus den Mitgliedstaaten, das die datenschutzrechtlichen Belange gegenüber den Entscheidungsträgern auf der


Im Zusammenhang mit der innerstaatlichen Umsetzung des Abkommens ist derzeit noch nicht entschieden, ob unter die daktyloskopischen Daten, auf die den US- Behörden der Zugriff eingeräumt werden soll, auch die Fingerabdruckdaten von Asylbewerbern oder Ausländern nach dem Aufenthaltsgesetz gefasst werden. Im Hinblick auf die Sensibilität daktyloskopischer Daten einerseits und das Fehlen eines angemessenen Datenschutzniveaus in den USA andererseits trete ich nachdrücklich dafür ein, den automatisierten Zugriff auf Fundstellendatensätze daktyloskopischer Daten von Straftätern zu begrenzen.

Die Ressortberatungen zum Entwurf des Umsetzungsgesetzes waren bei Redaktionsschluss noch nicht abgeschlossen.

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Uznzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden


Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungs- klauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.
13.5 Fluggastdaten

Die Verarbeitung dieser Daten stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung in erster Linie unbescholtener Bürgerinnen und Bürger dar. Den Nachweis, dass diese Daten unerlässlich sind, um den Terrorismus oder organisiertes Verbrechen wirksam zu bekämpfen, konnten weder die beteiligten Regierungen noch die EU-Institutionen erbringen.

Im Berichtszeitraum hatte ich mich vor allem mit entsprechenden Vorhaben auf EU-Ebene zu befassen. Bedeutsam waren insbesondere das zwischen den USA und der EU ausgehandelte dritte Abkommen zur Übermittlung von Fluggastdaten (Nr. 13.5.2) und der Vorschlag der Kommission für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdaten zu Strafverfolgungszwecken (Nr. 13.5.3).

13.5.1 Übermittlung von Flugpassagierdaten (PNR)

Globale Standards sind dringender denn je.

Flugreisende geben bei jeder Buchung eine Reihe von Daten an, die die Fluggesellschaft benötigt, um die Reise im gewünschten Umfang durchführen zu können. Dabei handelt es sich etwa um das Datum der Reise, Essenswünsche oder die Art der Bezahlung – Daten, die dann von den Fluggesellschaften in deren Buchungs- und Reservierungssystemen als PNR (Passenger Name Record)-Daten gespeichert werden (s. Kasten a zu Nr. 13.5.1).

Unterrichtung der Fluggäste


Großen Wert legt die Artikel-29-Gruppe darauf, dass die Passagiere nicht erst beim Einchecken über die Übermittlung der Daten unterrichtet werden, sondern spätestens dann, wenn die Flugbuchung erfolgt. Dabei soll genau aufgeführt werden, wer die Daten anfordern. Die Artikel-29-Gruppe betont, dass auf welcher Rechtsgrundlage die Übermittlung der einzelnen Datenelemente erfolgt und zu welchen Zwecken. Auch soll darüber informiert werden, für wie lange die Daten gespeichert werden, an welche Stellen sie weitergeleitet werden können und wo die Fluggäste weitergehende Auskünfte erhalten.


Ein zweiter Problemkreis ist das Datenschutzniveau im Empfängerstaat, insbesondere wenn dort keine Regelungen existieren, die den Anforderungen an einen angemessenen Datenschutzstandard entsprechen.

Auch in der EU gibt es Überlegungen, Passagierdaten im Kampf gegen Terrorismus und schwere Kriminalität zu nutzen (s. u. Nr. 13.5.3; vgl. Kasten b zu Nr. 13.5.1).

13.5.2 PNR USA

Das Datenschutzniveau des 2007 geschlossenen PNR-Abkommens mit den USA bleibt weit hinter dem vorherigen Abkommen zurück.


Nach wie vor ungeklärt ist die Frage der Umsetzung auf ein aktives Übermittlungsverfahren, das „Pull-Verfahren“, da die USA weiterhin die Daten zusätzlich noch aus den Buchungssystemen abrufen wollen (sog. „Pull-Verfahren“). Besonders unerfreulich ist, dass das neue Abkommen den betroffenen Reisenden keine subjektiven Rechte gewährt und dass jede Änderung der US-Gesetzgebung einseitig Auswirkungen auf das Datenschutzniveau des Abkommens haben kann. Auch wenn das Abkommen eine rechtliche Grundlage für die Übermittlung von Passagierdaten in die USA schafft, hätten sich die europäischen Datenschutzbehörden ein datenschutzfreundlicheres Abkommen gewünscht.

13.5.3 Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdaten (PNR-Daten) zu Strafverfolgungszwecken


Im Falle seiner Umsetzung würde dieser Vorschlag zu einer gigantischen Datensammlung sämtlicher die EU-Grenzen mit dem Flugzeug überquerenden Personen in einer Sicherheitsdatei führen, ohne dass die Betroffenen hierfür einen konkreten Anlass gegeben hätten. Eine Vorratsdatenspeicherung dieser Art würde gegen das in der EU-Grundrechtecharta garantierte Grundrecht auf Datenschutz verstoßen und wäre auch mit dem verfassungsrechtlich garantierten Recht auf informationelle Selbstbestimmung nicht vereinbar. In der Begründung wird nicht dargelegt, aus welchen Gründen die Verarbeitung von PNR-Daten unerlässlich für die Gewährleistung der Sicherheit in den Mitgliedstaaten ist. Insbesondere lässt der Vorschlag der Kommission außer Acht, dass bereits mit der Richtlinie 2004/82/EG (API-Richtlinie) die Fluggesellschaften verpflichtet wurden, den zuständigen Behörden der Mitgliedstaaten Fluggastdaten zu übermitteln (vgl. 20. TB Nr. 3.3.5). Mit dieser Richtlinie, deren Regelungen seit dem Jahr 2008 in innerstaatliches Recht umgesetzt sind (Nr. 13.5.4), ist ein Instrument zur Verbesse rung der Einreisekontrolle und zur Bekämpfung der illegalen Einwanderung geschaffen worden, das auch zur Bekämpfung des internationalen Terrorismus und sonstiger schwerwiegender Straftaten genutzt werden kann.


Vor diesem Hintergrund begrüße ich es zwar, dass die Bundesregierung noch einen Prüfvorbehalt aufrechterhält. Wegen seiner Unvereinbarkeit mit europäischem und nationalem Verfassungsrecht sollte sie den Rahmenbeschlussvorschlag jedoch in Gänze ablehnen.
Kasten zu Nr. 13.5.3

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008

Keine Vorratsspeicherung von Flugpassagierdaten


Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe „ins Blaue hinein“, also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr, sind unzulässig.


Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen und des Europäischen Datenschutzbeauftragten sowie der Artikel 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.


13.5.4 Umsetzung der Richtlinie 2004/82/EG zur Übermittlung von Fluggastdaten

Nach dem deutschen Umsetzungsgesetz müssen die Beförderungsunternehmen mehr Daten an die Bundespolizei übermitteln als von der Richtlinie vorgeschrieben.

Die Richtlinie 2004/82/EG über die Verpflichtung der Beförderungsunternehmen, auf Anfrage Angaben über beförderte Personen vorab an die mit der Personenkontrolle an den Außengrenzen der EU beauftragten nationalen Behörden zu übermitteln, ist in innerstaatliches Gesetz umgesetzt worden.

Im Gegensatz zum Rahmenbeschlussvorschlag der Kommission über die Verwendung von PNR-Daten zu Strafverfolgungszwecken (Nr. 13.5.3) zielt die Richtlinie (vgl. 20. TB Nr. 3.3.5) auf die Verbesserung der Grenzkontrollen und der Bekämpfung der illegalen Einwanderung ab. Der Umfang der zu erhebenden und zu übermittelnden Daten ist auf das dafür Notwendige begrenzt. Zudem sind die Daten nach Durchführung der Grenzkontrollen bei den zuständigen Behörden zu löschen. Zwar geht Deutschland bei der Umsetzung in innerstaatliches Recht hinaus (vgl. 21. TB Nr. 3.3.3). Im Laufe des Gesetzgebungsverfahrens konnte jedoch erreicht werden, dass von den ursprünglichen Plänen abgesehen wurde und nunmehr nur noch das „Geschlecht“ sowie die „Nummer des Visums“ von den Beförderungsunternehmen an die deutschen Grenzschutzbehörden als zusätzliche Daten über-

13.6 Listen der Vereinten Nationen und der Europäischen Union über Terrorverdächtige


Personen, die auf diesen Listen erscheinen, unterliegen umfangreichen Beschränkungen, die von Wirtschafts- und Finanzsanktionen über Einreiseverbote bis hin zum Einfrieren ihrer Gelder und anderer Vermögenswerte reichen. Ein Eintrag in die Listen greift damit nicht nur in das informationelle Selbstbestimmungsrecht ein. Er kann darüber hinaus gravierende existenzielle Folgen haben, wie z. B. die Verweigerung von Sozialleistungen.


Ich begrüße es, dass auf EU-Ebene ein Verfahren verabschiedet wurde, wonach gelistete Personen über die Aufnahme in die Listen informiert werden müssen, ihnen auf Antrag die Gründe für das Listing mitzuteilen sind und ihnen die Möglichkeit eingeräumt werden muss, dem Rat das Unterlag zu ihrer Entlastung vorzulegen.


13.7 Datenübermittlungen des Bundeskriminalamtes an Behörden der Russischen Föderation

Bei der Übermittlung personenbezogener Daten im polizeilichen Nachrichtenaustausch mit öffentlichen Stellen der Russischen Föderation und den damit zusammenhän-
genden Dokumentationspflichten beim Bundeskriminalamt (BKA) habe ich einzelne Mängel festgestellt.


Bei meinem Kontrollbesuch stellte sich auch heraus, dass die jeweilige Datenübermittlung zwar im jeweiligen Vorgang im Zusammenhang mit der laufenden Sachbearbeitung vermerkt wird. Dies wird aber der Aufzeichnungsmaßstab (§ 14 Absatz 7 Satz 3 BKAG) nicht gerecht. Sie stellt eine zusätzliche Verfahrenssicherung bei Datenübermittlungen an öffentliche und nicht-öffentliche Stellen in Drittstaaten dar und dient vor allem der datenschutzrechtlichen Eigen- und Fremdkontrolle. Vor diesem Hintergrund halte ich es für angebracht, die Aufzeichnungen über Datenübermittlungen an Drittstaaten gesondert zu führen und aufzubewahren – wie dies auch gemäß § 33 Absatz 2 BPolG vorgesehen ist –, um die betreffenden zugrunde liegenden Vorgänge in angemessener Zeit sachgerecht unter datenschutzrechtlichen Gesichtspunkten überprüfen zu können.


Bis Redaktionsschluss hat sich das BKA noch nicht abschließend zu den von mir aufgeworfenen Fragestellungen geäußert.

13.8 Die Europäische Frühjahrskonferenz

Die Konferenz der Datenschutzbeauftragten der Europäischen Union befasste sich vor allem mit Überlegungen zum Datenschutz in der Dritten Säule sowie mit neuen Herausforderungen angesichts weiterer Überwachungsmöglichkeiten von Reisenden.


13.9 Die Internationale Datenschutzkonferenz

Die Internationale Datenschutzkonferenz hat auch im Be-richtszeitraum wichtige Entschließungen zu aktuellen datenschutzpolitischen und datenschutzrechtlichen Frage-stellungen angenommen.


14 Andere Bereiche

14.1 Übermittlung von Gesundheitsdaten an Versicherungen

Auskünfte aus der Gesundheitsakte von Wehrpflichtigen und Berufssoldaten an externe Stellen dürfen nur bei Vorliegen einer differenzierten Schweigepflichterklärung erteilt werden.


Die § 29 Absatz 4 SG schließt grundsätzlich die Weitergabe dieser sensiblen Gesundheitsdaten an Stellen außerhalb des Geschäfts bereiches des Bundesministeriums der Ver-teidigung aus. Sie ist nur möglich, wenn der Betroffene selbst eine entsprechende Schweigepflichterklärungsanfragen erteilt. An die Wirksamkeit einer solchen Erklärung sind aber strenge Maßstäbe anzulegen.

Wie ich aus Eingaben weiß, war vielen Soldaten, insbe-sondere Wehrpflichtigen, aufgrund der oftmals pauschalen Formulierung nicht bewusst, dass die Versicherungen hierdurch auch Auskunft über ihre Andernach geprüften Gesundheitsdaten erhalten haben, ebenso, dass diese Daten überhaupt derart lange gespeichert sind. Hierdurch konnte die Rechtmäßigkeit der Übermittlung der Daten an Versicherungen in Zweifel gezogen werden. Schließlich sind die Versicherungen verpflichtet, nach der sachgerechten Verarbeitung der Daten und dem datenschutzrechtlichen Schutz der Betroffenen die überlassenen Daten zu löschen.

Diese Praxis der Auskunftserteilung widerspricht dem Beschluss des Bundesverfassungsgerichts vom 23. Okt-ober 2006 (1 BvR 2027/02), demzufolge eine formularmäßige und zum Teil sehr allgemein umschriebene Erklä- rung das Interesse des Betroffenen an einem wirksamen informationellen Selbstschutz erheblich beeinträchtigt (vgl. 21. TB Nr. 9.6).
Das BMVg hat ein neues Formular einer Schweigepflichtentbindungserklärung nach den Vorgaben des Gerichts erstellt. Das Institut in Andernach erteilte inzwischen nur noch Auskünfte bei Verwendung dieses Formulars. Die neue Praxis ist datenschutzrechtlich nicht zu beanstanden.

14.2 Unzweckmäßiger Datenschutz in einer Auslandsvertretung

Die Prüfung einer Botschaft im Frühjahr 2008 machte eine Reihe von erheblichen Defiziten deutlich und führte zu Beanstandungen.

Im 20. TB (Nr. 23.1 und 23.2) hatte ich über Mängel bei der Aktenführung in einer Botschaft und Probleme bei der Wahrung der Diskretion in Auslandsvertretungen berichtet. Die vor diesem Hintergrund erfolgte eingehende Prüfung einer Botschaft im Berichtszeitraum erbrachte eine Reihe datenschutzrechtlich kritischer Feststellungen und führte zu einigen Beanstandungen. Das Auswärtige Amt hat hierauf rasch reagiert und ist in den meisten Punkten meinen Anregungen bereits gefolgt.

Der mit meiner Unterstützung 2002 in Kraft getretene „Runderlass Datenschutz“ (s. 20. TB Nr. 23.1) regelt für alle Auslandsvertretungen die Umsetzung einschlägiger datenschutzrechtlicher Vorgaben, etwa des BDSG. Leider zeigte die Kontrolle, dass die konkrete Umsetzung vor datenschutzrechtlichen Vorgaben, etwa des BDSG. Leider zeigte die Kontrolle, dass die konkrete Umsetzung vor Ort unzureichend war:


Ich habe die Beauftragung des Kanzlers mit dem Amt des behördlichen Datenschutzbeauftragten als Verstoß gegen § 4f Absatz 2 BDSG und damit erheblichen Mangel beanstandet und das AA gebeten, alle Auslandsvertretungen in diesem Sinne zu überprüfen. Das AA hat inzwischen einen neuen Datenschutzbeauftragten in der geprüften Botschaft ernannt und überdies im Hinblick auf die Größe der Botschaft auf meine Anregung hin auch einen Stellvertreter.


Nach § 18 Absatz 2 Satz 2 BDSG haben öffentliche Stellen für ihre automatisierten Verarbeitungen die Angaben nach § 4e BDSG z. B. die Zweckbestimmung der Datenerhebung und -verwendung, sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Da dies in der Botschaft nicht erfolgt war, habe ich auch hier eine Beanstandung ausgesprochen. Das AA ist nun dabei, das vom Bundesministerium der Finanzen unter meiner Beteiligung hierfür entwickelte Verfahren DATSCHA (Datenschutzanwendung in der Bundesfinanzverwaltung) in den Auslandsvertretungen zu nutzen.

Das AA hat zugesagt, die Umsetzung des Runderlasses ab sofort intensiv zu überprüfen und entsprechende Schulungen in den Auslandsvertretungen durchzuführen. Ich werde diese Maßnahmen aufmerksam begleiten.

- Das Problem der Wahrung der Diskretion bei der mündlichen Darstellung von Sachverhalten durch betroffene Antragsteller ist, obwohl vom AA zugesagt (s. 20. TB Nr. 23.2), nach wie vor nicht gelöst. In der geprüften Botschaft sind sowohl in der Visa-Stelle als auch in der Botschaftszentrale Räume mit mehreren Schaltern eingerichtet, die den Besuchern gleichzeitig als Warteräume dienen. Umstehende sind in der Lage, den Gesprächen, die entweder über Telefonhörer oder Mikrofone geführt wurden, zu beträchtlichen Teilen zu folgen. Selbst bei vorhandenen Diskretionsräumen, auf die im Übrigen nicht hingewiesen wurde, waren zumindest in der Nähe der Türen die Gespräche mitzuhören.


15 Aus meiner Dienststelle

15.1 Konferenz der Datenschutzbeauftragten des Bundes und der Länder


sind zudem über meinen Internet-Auftritt unter www.bfdi.bund.de abrufbar.

15.2 Europäischer Datenschutztag

Zahlreiche Aktivitäten anlässlich des vom Europarat im Jahr 2007 ausgerufenen Europäischen Datenschutztages


### 15.4 Bad Godesberger Symposien zum Datenschutz in der Telekommunikation und im Internet

Die Reihe der Herbstsymposien des BfDI wurde fortgesetzt.

Die Funktion der Suchmaschinen als digitale Gatekeeper, also „Torhüter“ der digitalen Welt, und damit ihre zungangssteuernde und potentiell meinnungshemmende Wirkung beleuchtete der Leipziger Mediawissenschaftler Professor Marcel Machill beim VIII. Symposium im November 2007. Für ein Impulsreferat zur Online-Durchsuchung konnte der frühere Bundesinnenminister Gerhard Rudolf Baum gewonnen werden, der vor dem Bundesverfassungsgericht erfolgreich die Regelung der Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz angegriffen und damit eine der grundlegenden Karlsruher Entscheidungen zur Fortbildung des Datenschutzrechts angestoßen hat (s. hierzu u. a. Nr. 2.1, 4.1 ff.). Die Frage nach der verfassungsrechtlichen Entwicklung und der Herausbildung neuer Grundrechte griffen der Hessische Datenschutzbeauftragte Professor Michael Ronellenfitsch und Dr. Klaus Abmeier aus dem Bundesministerium der Justiz in ihren Referaten auf.

Ich habe beim VIII. Symposium auf die Bedrohung der Privatsphäre hingewiesen, die exemplarisch durch die Ausweitung der Telekommunikationsüberwachung, die
Online-Durchsuchung und die Vorratsdatenspeicherung belegt wird. Die Privatsphäre ist heute im Kern bedroht. Effektive Gegenstrategien müssen deshalb bei der Technologie, aber auch bei rechtlichen, politischen und wirtschaftlichen Steuerungsmöglichkeiten ansetzen. Im Ergebnis geht es dabei auch um die Entwicklung einer globalen Ethik des Informationszeitalters, in deren Mittelpunkt die Bewahrung und Entwicklung der individuellen Selbstbestimmung steht.

Das IX. Symposium im November 2008 befasste sich u. a. mit der Marktentwicklung vor dem Hintergrund der Revision der europarechtlichen Vorgaben zum Telekommunikationsrecht sowie Fragen des Datenschutzes und der Kundenakquise im Mobilfunk.


15.5 Zusammenarbeit mit den behördlichen Datenschutzbeauftragten

Der von mir initiierte regelmäßige Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten der obersten Bundesbehörden liefert wichtige Anregungen


Neben einer ausführlichen Unterrichtung über aktuelle Entwicklungen im Datenschutzrecht, insbesondere über BDSG-Änderungen, neue Gesetzentwürfe sowie Gerichtsentscheidungen und ihre Auswirkungen war die Situation der behördlichen Datenschutzbeauftragten in ihren jeweiligen Dienststellen ein Schwerpunkt. Dabei wurden Erfahrungen zum Arbeitsanfall bzw. zum Umfang der Freistellung sowie der Unterstützung durch weitere Mitarbeiterinnen und Mitarbeiter ausgetauscht. Die behördlichen Datenschutzbeauftragten berichteten über eine allgemein zufrieden stellende Situation, auch wenn in

Einzelfällen der Eindruck entstanden sei, dass infolge von Einsparungen im Personalaufwand Belange des Datenschutzes bisweilen nicht ausreichend berücksichtigt würden. Aus der Tatsache, dass es nur vereinzelt zu Problemen bei der Freistellung der behördlichen Datenschutzbeauftragten gekommen ist, kann geschlossen werden, dass zumindest die obersten Bundesbehörden der von der Bundesregierung anerkannten Pflicht zur teilweisen oder völligen Freistellung von anderen Aufgaben (vgl. 20. TB Nr. 2.4; 21. TB Nr. 2.6) gerecht werden.

Erörtert wurden auch die organisatorische Zuordnung in der jeweiligen Dienststelle und Fragen der Kompatibilität der Funktion als Beauftragter für den Datenschutz mit gleichzeitig übertragenen anderen Aufgaben. Beim Thema Datensicherheit standen das neue Datenschutzkapitel im IT-Grundschatzkatalog des Bundesamts für Sicherheit in der Informationstechnik sowie Fragen des datenschutzgerechten Löschens von Datenträgern im Vordergrund (vgl. 21. TB Nr. 4.8 sowie o. Nr. 8.3). Weitere wichtige Themen waren die Ausgestaltung eines Verfahrens zur Leistungsfeststellung im Rahmen des neuen Bundesbesoldungsgesetzes und rechtliche Fragen im Zusammenhang mit der Aufgabenverlagerung auf externe Stellen durch Outsourcing oder Auftragsdatenverarbeitung (vgl. 21. TB Nr. 2.5 sowie o. Nr. 2.5).

Ich werde die behördlichen Datenschutzbeauftragten in ihrer wichtigen Funktion bei der Verwirklichung des Datenschutzes in ihrer Dienststelle auch weiterhin aktiv unterstützen, sowohl durch Beratungen im Einzelfall als auch durch Fortsetzung des regelmäßigen Erfahrungsaustausches.

15.6 Zusammenarbeit mit den Aufsichtsbehörden


Der Düsseldorfer Kreis hat im Berichtszeitraum nicht nur zu den beiden Gesetzesvorhaben der Bundesregierung zur Änderung des BDSG Stellung genommen, sondern auch ein Positionspapier zum internationalen Datenverkehr und eine Handreichung zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung beschlossen (abrufbar auf meiner Website unter www.bfdi.bund.de). Daneben hat er eine Reihe weiterer wichtiger Beschlüsse gefasst (vgl. Kasten zu Nr. 15.6).

Kasten zu Nr. 15.6

Beschlüsse des Düsseldorfer Kreises in den Jahren 2007/2008:

- Erhebung von Positivdaten zu Privatpersonen bei Auskunfteien
- Mahnung durch Computeranruf
- Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte
- Gesetzesinitiative der Bundesregierung zu Auskunftseiten und Scoring
- Internet-Portale zur Bewertung von Einzelpersonen
- Keine fortlaufenden Bonitätsauskünfte an den Verandsandel
- Datenschutzkonforme Gestaltung sozialer Netzwerke
- Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet
- Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adresshandel, Werbung und Datenschatzaudit

abrufbar über meine Website unter www.bfdi.bund.de

15.7 Die Internationale Datenschutzkonferenz 2008


15.8 Öffentlichkeitsarbeit

Neue Informationsmaterialien und Gespräche vor Ort: Information und Beratung von Bürgerinnen und Bürgern

Der Stellenwert des Datenschutzes nimmt auf Grund immer umfassenderer Datensammlungen und der mit den technologischen Entwicklungen einhergehenden Risiken für die Privatsphäre stetig zu. Deshalb ist es natürlich, dass sich immer mehr Bürgerinnen und Bürger mit Fragen an mich wenden und um Empfehlungen bitten, wie Sie Ihre persönlichen Daten vor Missbrauch schützen können.

Sie nutzen verstärkt die Möglichkeit, sich auf meiner Website (www.bfdi.bund.de) zu informieren. Die Neugestaltung dieses Internet-Angebots ist gut angenommen worden. Das belegen die steigenden Nutzerzahlen (s. Kasten zu Nr. 15.8).


Neben meinem Internet-Angebot stelle ich den anfragenden Bürgerinnen und Bürgern die Informationsschriften und Faltblätter selbstverständlich auch weiterhin in Papierform zur Verfügung.

Im Berichtszeitraum wurde eine neue Info 2 zum Informationsfreiheitsgesetz veröffentlicht. Diese Broschüre soll allen Interessierten die Möglichkeit geben, sich schnell und umfassend über ihre Rechte auf freien Zugang zu amtlichen Informationen öffentlicher Stellen zu informieren und diese zielgerichtet wahrzunehmen. Sie enthält neben Erläuterungen zum Informationsfreiheitsgesetz des Bundes und praktischen Tipps für die Antragstellung eine Zusammenstellung der Informationsfreiheitsgesetze des Bundes und – soweit vorhanden – der Länder, der entsprechenden Regelungen der Europäischen Union sowie weiterer damit in Zusammenhang stehender Rechtsvorschriften wie das Umweltinformationsgesetz und das Verbraucherinformationsgesetz.


Daneben sind im Berichtszeitraum einige neue Arbeitshilfen zu technischen Themen erschienen, wie zum Protection Profile – Software zur Verarbeitung von personenbezogenen Bitdaten und datenschutzrechtliche Grundlagen bei der Auftragsdatenverarbeitung/Outsourcing in der öffentlichen Verwaltung.


Am Tag der offenen Tür der Bundesregierung war der BfDI wieder mit einem Informationsstand vertreten, um die Bürgerinnen und Bürger vor Ort über die Themen Datenschutz und Informationsfreiheit zu informieren und Fragen zu beantworten. Hier bestand die Gelegenheit, sowohl Besucherinnen und Besucher auf die Gefahren und Chancen bei der Datenverarbeitung hinzuweisen, sie auf ihre Rechte aufmerksam zu machen und für die Themen Datenschutz und Informationsfreiheit zu sensibilisieren, als auch Fragen zu beantworten und über aktuelle Frage-
stellungen mit den Besucherinnen und Besuchern zu diskutieren. Seit 2002 präsentiere ich meine Aufgaben und mein Tätigwerden am Tag der offenen Tür der Bundesregierung und jedes Jahr kommen mehr Bürgerinnen und Bürger gezielt an meinen Stand, um ihre Fragen zu stellen und ihre Anliegen vor Ort zu diskutieren.

Insbesondere trägt meine Pressestelle mit dazu bei, dass Ereignisse mit Datenschutzbezug meine Bewertung finden und über die Medien in die breite Öffentlichkeit gebracht werden, um dort Beachtung zu finden. Dies geschicht u. a. durch Pressemithteilungen, die bei Bedarf herausgegeben werden und die oft auch nützliche Tipps für den täglichen Umgang mit Daten beinhalten.

Ohne die zahlreichen unmittelbaren Kontakte zu Pressevertretern aller Medien wäre die Sensibilisierung der Öffentlichkeit für das Thema „Datenschutz“ ein wesentlich schwierigeres Unterfangen. Ich lege daher großen Wert darauf, dass die Pressestelle den Vertreterinnen und Vertretern der Medien mit Rat und Tat zur Verfügung steht.

Ebenso tragen sicherlich meine Artikel, die ich zu verschiedenen Themenbereichen, wie z. B. der Videointüberwachung oder dem neuen BKA-Gesetz, für die Tagespresse und Fachpublikationen geschrieben habe, dazu bei, die Wahrnehmung des Datenschutzes in der Öffentlichkeit zu stärken.

Kasten zu Nr. 15.8

### Nutzerzahlen der Internet-Seite www.bfdi.bund.de:

<table>
<thead>
<tr>
<th></th>
<th>2008</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seitenaufrufe (gesehener Traffic)</td>
<td>3.847.543</td>
<td>2.353.119</td>
</tr>
<tr>
<td>Seitenaufrufe (nicht gesehener Traffic)*</td>
<td>3.528.632</td>
<td>3.926.474</td>
</tr>
<tr>
<td>Seitenaufrufe gesamt</td>
<td>7.376.175</td>
<td>6.279.593</td>
</tr>
</tbody>
</table>

* Nicht gesehener Traffic ist Traffic, welcher im Wesentlichen von Robots, insbesondere zur automatisierten Auswertung durch Suchmaschinen verursacht wurde.

15.9 Mehr Präsenz in der Bundeshauptstadt

**Mein Verbindungsbüro in Berlin hat sich bereits nach kurzer Zeit bewährt.**


15.10 BfDI als Ausbildungsbehörde

**Referendare und Praktikanten**

Auch in den letzten zwei Jahren war erneut großes Interesse an Praktikumsaufenthalten in meiner Dienststelle festzustellen. Insbesondere von Studierenden der Rechtswissenschaften und Rechtsreferendaren, die sich für Fragen des Datenschutzes und der Informationsfreiheit interessierten und praktische Kenntnisse erwerben wollten.


15.11 Zusätzliches Personal dringend erforderlich

**Gesetzliche Aufgaben können mit dem vorhandenen Personal nicht mehr angemessen und in vollem Umfang erledigt werden.**

In meiner Dienststelle ist der Aufgaben- und Arbeitsanfall seit Jahren kontinuierlich stark angestiegen. Die personelle Ausstattung hat mit dieser Entwicklung nicht Schritt gehalten, so dass im Ergebnis die Zahl der Planstellen und Stellen, die für die Erledigung der gesetzlichen Aufgaben zur Verfügung stehen, inzwischen deutlich zu gering bemessen ist. 50 Planstellen und 17 Stellen für Tarifbeschäftigte stehen haushaltsmäßig meiner Dienststelle zur Verfügung. Hiermit sind rd. 20 Funktionsstellen und Stellen, die für die Erledigung der gesetzlichen Aufgaben zur Verfügung stehen, inzwischen deutlich zu gering bemessen. 50 Planstellen und 17 Stellen für Tarifbeschäftigte stehen haushaltsmäßig meiner Dienststelle zur Verfügung. Hiermit sind rd. 20 Funktionen der Infrastruktur (überwiegend einfacher und mittlerer Dienst) und der IT-Administration (in Zugleichfunktion mit Datenschutzaufgaben) stellenmäßig unterlegt. Obwohl sich die Zahl der Bürgereingaben wie auch die Gesamtanliegen von Jahr zu Jahr vervielfacht haben, muss dieser enorme Anstieg mit dem vorhandenen Personal bewältigt werden (s. Kasten zu Nr. 15.11).
Durch die geschilderte Situation sind deutlich spürbare Engpässe und Verzögerungen bei der Wahrnehmung gesetzlicher Aufgaben im Datenschutz und auch im IFG-Bereich entstanden. Eine strikte Priorisierung hat dazu geführt, dass einzelne Bereiche zurzeit nicht angemessen „betreut“ werden können; ein Rückgang der Kontrolldichte ist die Folge. Dies kann – auch vor dem Hintergrund aktueller Ereignisse im Bereich des Datenschutzes und der ständig wachsenden Zahl datenschutzrelevanter IT-Verfahren – so nicht weiter hingenommen werden. Die Zahl und der Umfang datenschutzrechtlicher Prüfungen sind zu erweitern, damit Umsetzungsdefizite des Datenschutzrechts abgebaut und zunehmenden Risiken Rechnung getragen werden kann. Es darf dabei auch nicht außer Acht gelassen werden, dass die neue Qualität der Datenverarbeitung auf europäischer Ebene (Stichworte sind hier z. B. die Dienstleistungsrichtlinie, Nr. 3.4.1 und Schengen Nr. 13.3.4) zusätzliche Anforderungen an die datenschutzrechtliche Begleitung der Vorhaben und an die Kontrolle der Einhaltung gesetzlicher Vorgaben stellen.

Dienststelleninterne Maßnahmen konnten die Lage nur ansatzweise entspannen: So wurde z. B. ein Servicebüro eingerichtet, das den Referaten u. a. für die Bearbeitung von Eingaben unterstützend zur Verfügung steht und so zu einer Entlastung beiträgt. Zudem wurden im Rahmen der Optimierung der Ablauf- und Aufbauorganisation in der Dienststelle des BfDI und zur besseren Nutzung vorhandener Personalressourcen Organisationseinheiten umstrukturiert, Projektgruppen gebildet und ein Verbindungsbüro in Berlin eingerichtet (s. unter Nr. 15.9).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Anzahl</td>
<td>1541</td>
<td>2000</td>
<td>1647</td>
<td>1927</td>
<td>2376</td>
<td>2449</td>
<td>3067</td>
<td>3295</td>
<td>4309</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Anzahl</td>
<td>11320</td>
<td>16267</td>
<td>11594</td>
<td>15940</td>
<td>18876</td>
<td>20020</td>
<td>24132</td>
<td>25056</td>
<td>30303</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Jahr</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anzahl</td>
<td>6555</td>
<td>6031</td>
<td>6686</td>
<td>5997</td>
<td>6872</td>
</tr>
</tbody>
</table>
16 Wichtiges aus zurückliegenden Tätigkeitsberichten

1. 21. TB Nr. 7.1.1 zum Gesetz zur Umsetzung aufenthalts- und asylrechtlicher Richtlinien der Europäischen Union


2. 20. TB Nr. 6.2.3; 21. TB Nr. 7.1.4 zum europäischen Visa-Informationssystem (VIS):


3. 21. TB Nr. 7.1.3 zur Datenerhebung zur Forschungszwecken ohne Rechtsgrundlage:

Mittlerweile liegt der von mir angemahnte Entwurf des Gesetzes zur Verbesserung der Bekämpfung von Visumsmisbrauch und Schleusungskriminalität vor, in dessen Rahmen in § 24a AZRG-E die Verwendung personenbezogener Daten für wissenschaftliche Zwecke geregelt werden soll.

Datenschutzrechtliche Bedenken bestehen hiergegen nicht. Daher hielt ich im Vorgriff auf diese Forschungsklausel es für vertretbar, das Projekt durchzuführen.

4. 16. TB Nr. 5.8 zum Suchdienstedatenschutzgesetz (SDDSAG):


5. 21. TB Nr. 8.3 zum Entwurf des Zweiten Gesetzes zur Änderung des Vierten Buches Sozialgesetzbuch und anderer Gesetze, wie z. B. des Schwarzarbeitsbekaufungs- und datenschutzrechtlichen Bedenken gegen die in § 17 Absatz 1 Nummer 1 SchwarzArbG-E vorgesehene Erweiterung des Zugriffs der Polizeivollzugsbehörden des Bundes auf die zentrale Datenbank werden von mir nach ergänzenden Ausführungen in der Begründung zur Erforderlichkeit dieser Zugriffe nicht mehr geteilt. Dort wird u. a. ausgeführt, dass § 17 Absatz 1 Nr. 3 SchwarzArbG den Polizeibehörden...

6. 20. TB Nr. 16.1.3; 21. TB Nr. 13.5.3 zum Erhe- bungs- und Leistungssystems A2LL bei der BA:


7. 21. TB Nr. 13.5.5 zur unzulässigen Datensammlung der BA über die Nutzer der BA-Internet-Plattform:


8. 21. TB Nr. 19.2 zum Zentralen Vorsorgeregister bei der Bundesnotarkammer:


9. 21. TB Nr. 15.1 zum Online-Angebot „Öffentliche Petition“:


10. 21. TB Nr. 16.1 zum Projekt HERKULES:

Mit dem Projekt HERKULES will das Bundesminis- terium der Verteidigung (BMVg) nahezu seine gesamte Informationstechnik outsourcen. Die techni- schen und organisatorischen Schutzmaßnahmen sol- len im Datenschutzkonzept HERKULES und dem übergreifenden IT-Sicherheitskonzept HERKULES spezifiziert werden. Beides soll mir nach Fertigstel- lung zugeleitet werden.

Das Verfahren werde ich weiterhin aufmerksam be- gleiten.

11. 21. TB Nr. 16.2 zur Privatisierung der bundeseige- nen Kleiderkasse:

Ich hatte darüber berichtet, dass bei der Privatisie- rung der bundeseigenen Kleiderkasse der Bundes- wehr umfangreiche Datenbestände von aktiven und ehemaligen Bundeswehrangehörigen an die privat- rechtlich organisierten Nachfolgegesellschaften über- mittelt worden sind, ohne im Vorfeld die Erforder- lichkeit hierfür sorgfältig zu prüfen. Die Daten waren dann zu Werbezwecken eingesetzt worden, wogegen sich Petenten gewandt hatten. Meiner Aufforderung, die Mängel im Umgang mit den Kundendaten der ehemaligen Kleiderkasse zu beheben, ist das BMVg durch die Erstellung eines Datenschutzkonzeptes, was sich derzeit noch in der Prüfung befindet, nach- gekommen.

12. 21. TB Nr. 17.2 zum Vertragslosen Zustellungsver- kehr:

13. 21. TB Nr. 13.1.3 zu Entlassungsberichten aus Rehabilitationseinrichtungen:


14. 20. TB Nr. 10.3.2; 21. TB Nr. 14.3 zu EPOS 2.0:


15. 21. TB Nr. 14.2 zum Dienstrechtsneuordnungsge setz:


16. 21. TB Nr. 11.2 zum Express- und Paketzustellungsdienst UPS:


17. 21. TB Nr. 12.6 zur Übermittlung flugmedizinischer Daten an das Luftfahrt-Bundesamt (LBA):


Ich werde die Entwicklung weiterhin aufmerksam verfolgen und mich dafür einsetzen, dass ein Gleichgewicht zwischen der notwendigen Fachaufsicht und dem schutzwürdigen Interesse des Einzelnen hergestellt wird.

18. 21. TB Nr. 12.2 ff. zu Telematikverfahren für Kraftfahrzeuge:

 Zu den Telematikverfahren für Kraftfahrzeuge – E-Call, Event Data Recorder, Pay as You Drive – haben sich in der Zwischenzeit keine wesentlichen neuen Entwicklungen ergeben. Bezüglich des automatischen Notrufsystems E-Call geht die Europäische Kommission nach wie vor davon aus, dass es ab Septem-

19. 21. TB Nr. 7.6 zu Wissenschaftsservern:

20. 21. TB Nr. 9.4 zu SWIFT:

21. 21. TB Nr. 5.2.4.1 zur Verarbeitung erkenntnisdienstlicher Unterlagen im Bundeskriminalamt:

22. 21. TB Nr. 5.2.7 zur Geldwäsche:

23. 21. TB Nr. 5.4.1 zum Zollfahndungsdienstegesetz:

Den verfassungsrechtlichen Vorgaben zur Gewährleistung des Kernbereichs privater Lebensgestaltung wurde dabei allerdings nicht in vollem Umfang
Rechnung getragen. Quasi als Vorbild für die spätere BKA-Gesetzesnovelle (Nr. 4.3.1) wird der Kernbereichsschutz auch in diesem Gesetz insofern unzulässig verkürzt, als eine präventiv-polizeiliche Telekommunikationsüberwachung nur unzulässig ist, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass allein kernbereichsrelevante Kommunikationsinhalte erfasst werden. Zudem fehlen kernbereichsschützende Regelungen in Zusammenhang mit den in §§ 18 ff. ZfDG normierten verdeckten Datenerhebungsbefugnissen völlig.


24. 21. TB Nr. 6.2 zur akustischen Wohnraumüberwachung:

Ich habe bereits über die am 1. Juli 2005 in Kraft getretene Neuregelung der akustischen Wohnraumüberwachung in der StPO berichtet. Inzwischen hat das BVerfG die neuen Vorschriften in § 100c StPO zum Schutz des Kernbereichs privater Lebensgestaltung für verfassungsgemäß erklärt (Beschluss vom 11. Mai 2007, 2 BvR 543/06).


25. 21. TB Nr. 10.3 zur unterdrückten Rufnummer:


Hinweise für die Ausschüsse des Deutschen Bundestages

Nachfolgend habe ich dargestellt, welche Beiträge dieses Berichtes für welchen Ausschuss von besonderem Interesse sein könnten:

Auswärtiger Ausschuss
13.1; 13.5 ff.; 13.6; 13.8; 13.9; 14.2

Innenausschuss
2.1 bis 2.9; 3.1; 3.2.1 bis 3.2.5; 3.4.4 bis 3.4.7; 4.1.; 4.2.1; 4.8.3; 5.2 bis 5.5; 6; 6.3; 6.3.1 f.; 6.5; 6.8; 6.9; 7.1 bis 7.3; 7.6; 7.10; 7.11; 11.2; 11.3; 13.3.1 bis 13.3.2; 13.3.6; 13.5.3; 13.6; 16.1 bis 16.4

Sportausschuss
5.9

Rechtsausschuss
2.1 bis 2.6; 2.8 bis 2.10; 3.1; 3.2.1 bis 3.2.5; 3.4.4 bis 3.4.7; 4.1; 4.5; 5.1; 6.3.1 f.; 6.9; 7.1 bis 7.4; 7.6; 7.10; 7.11; 8; 13.2; 13.3.1; 13.5 ff.; 13.6; 16.8; 16.12

Finanzausschuss
6.4; 9.1 bis 9.5; 16.5

Ausschuss für Wirtschaft und Technologie
2.2 bis 2.6; 2.8; 3.1; 3.2.1 bis 3.2.5; 3.4.1; 3.4.4 bis 3.4.7; 6; 6.2; 6.9; 7.1 bis 7.2; 7.9; 7.11; 8; 13.2.3

Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz
2.2 bis 2.6; 2.8; 3.1; 3.4.4 bis 3.4.5; 3.4.7; 6; 6.8; 8.5

Ausschuss für Arbeit und Soziales
7.6; 10.4; 10.5.1 bis 10.5.4; 11.1; 11.3; 11.4; 16.6 f.

Verteidigungsausschuss
14.1; 16.10 ff.

Ausschuss für Familie, Senioren, Frauen und Jugend
2.9; 7.3

Ausschuss für Gesundheit
6.1; 6.1.2; 6.2; 10.1 bis 10.4; 16.13

Ausschuss für Verkehr, Bau und Stadtentwicklung
12.1

Ausschuss für Bildung, Forschung und Technikfolgenabschätzung
6; 6.3; 6.8; 8; 8.1 bis 8.5

Ausschuss für die Angelegenheiten der Europäischen Union
6; 8; 13.1 bis 13.2; 13.2.1; 13.5 ff.; 13.8

Ausschuss für Kultur und Medien
3.2.1 bis 3.2.2; 5.5; 5.7; 7.1 bis 7.3; 7.6

Ausschuss für Kultur und Medien – Unterausschuss „Neue Medien“ –
6; 6.3; 6.8; 7.1 bis 7.3; 8; 8.1 bis 8.5;
Anlage 2

Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche

Auswärtiges Amt
- Botschaft

Bundeskanzleramt (einschließlich Beauftragter für Kultur und Medien)
- Bundesnachrichtendienst
- Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (Zentrale und zwei Außenstellen)

Bundesministerium des Innern
- Ministerium
- Bundesverwaltungsamt
- Statistisches Bundesamt
- Technisches Hilfswerk
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
- Bundesinstitut für Sportwissenschaft
- Bundeskriminalamt (Wiesbaden, Meckenheim und Berlin)
- Bundespolizeidirektion
- Bundespolizeiamt Halle/S
- Bundespolizeiamt Flughafen Frankfurt/Main
- Bundesamt für Verfassungsschutz

Bundesministerium der Justiz
- Bundesamt für Justiz
- Bundesnotarkammer
- Generalbundesanwalt

Bundesministerium der Finanzen
- Bundeszentralamt für Steuern/Informationszentrale für steuerliche Auslandsbeziehungen
- Bundesanstalt für Finanzdienstleistungsaufsicht
- Deutsche Bundesbank

Bundesministerium für Arbeit und Soziales
- Ministerium
- Deutsche Rentenversicherung Bund
- Bundesagentur für Arbeit
- Agentur für Arbeit (Jobbörse)

Bundesministerium der Verteidigung
- Ministerium
- Militärischer Abschirmdienst

Bundesministerium für Familie, Senioren, Frauen und Jugend
- Bundesamt für den Zivildienst

Bundesministerium für Gesundheit
- Bundesversicherungsamt
- Robert-Koch-Institut

Bundesministerium für Verkehr, Bau und Stadtentwicklung
- Ministerium
- Luftfahrt-Bundesamt
- Kraftfahrt-Bundesamt
- Maritimes Sicherheitszentrum

Bundesministerium für Wirtschaft und Technologie
- Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
- Ministerium

Deutsche Post AG
- Zentrale
- Briefzentrum Köln
- DHL Zentrale
- Tochterunternehmen Deutsche Post Adress GmbH und Deutsche Post Direkt GmbH

Neue Postdienstunternehmen
- Hermes Logistik Service, Außenstelle Aachen
- TNT Express und TNT Post (Thomas Nationwide Transport)
- PIN Mail AG, Berlin

Telekommunikationsunternehmen
- Deutsche Telekom AG
<table>
<thead>
<tr>
<th>Kabel Deutschland GmbH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobilcom Communicationstechnik GmbH</td>
</tr>
<tr>
<td>O2 (Germany) GmbH &amp; Co. OHG</td>
</tr>
<tr>
<td>O2 (Germany) Service GmbH</td>
</tr>
<tr>
<td>Betamax GmbH &amp; Co. KG</td>
</tr>
<tr>
<td>Arcor AG &amp; Co. KG</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sonstige</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innungskrankenkasse Hamburg</td>
</tr>
<tr>
<td>Innungskrankenkasse Weser-Ems</td>
</tr>
<tr>
<td>BARMER Ersatzkasse</td>
</tr>
<tr>
<td>Wirtschaftsunternehmen wegen Verfahren zur Sicherheitsüberprüfung</td>
</tr>
</tbody>
</table>
Anlage 3

Übersicht über Beanstandungen nach § 25 BDSG

### Auswärtiges Amt
- Verstoß einer Auslandsvertretung gegen § 4f Absatz 2 Satz 1 BDSG wegen Bestellung des Kanzlers der Botschaft (u. a. Zuständigkeit für Personalangelegenheiten) zum behördlichen Datenschutzbeauftragten (s. Nr. 14.2)
- Verstoß einer Auslandsvertretung gegen § 18 Absatz 2 Satz 1 BDSG wegen mangelnder Führung des Verzeichnisses der Datenverarbeitungsanlagen (s. Nr. 14.2)
- Verstoß einer Auslandsvertretung gegen § 18 Absatz 2 Satz 2 i. V. m. § 4e BDSG wegen fehlender schriftlicher Angaben zur Zweckbestimmung der Datenerhebung und -verwendung sowie der Rechtsgrundlage der Datenerhebung (s. Nr. 14.2)

### Bundesministerium des Verteidigung
- Verstoß des Militärischen Abschirmdienstes gegen § 24 Absatz 4 BDSG wegen fehlender Mitwirkung (s. Nr. 4.7.2)

### Bundesministerium für Wirtschaft und Technologie
- Verstoß der PIN Group AG gegen die Mitwirkungspflicht nach § 24 Absatz 4 BDSG (s. Nr. 3.3.2)

### Gesetzliche Krankenkassen
Drei Beanstandungen wegen:
- Verstoß gegen das in § 35 SGB I normierte Sozialgeheimnis
- Verstoß gegen § 284 Absatz 3 SGB V
- Verstoß gegen die Vorschriften des § 78a SGB X und der Anlage zu § 78a SGB X (s. Nr. 10.2.4)

Zwei Beanstandungen wegen:
- Verstoß gegen das in § 35 SGB I normierte Sozialgeheimnis
- Verstoß gegen die Vorschriften des § 78a SGB X und der Anlage zu § 78a SGB X (s. Nr. 10.2.4)

### Sonstige
- Verstoß gegen Sicherheitsüberprüfungen außerhalb des SÜG wegen fehlender Rechtsgrundlage für eine Zuverlässigkeitsüberprüfung (s. Nr. 4.8.3.2)
Beschlussempfehlung und Bericht
des Innenausschusses (4. Ausschuss)

zu der Unterrichtung durch den Bundesbeauftragten für den Datenschutz
– Drucksache 15/5252 –

Tätigkeitsbericht 2003 und 2004 des Bundesbeauftragten für den Datenschutz
– 20. Tätigkeitsbericht –

A. Problem
Der 20. Tätigkeitsbericht gibt einen Überblick über die Schwerpunkte der Arbeit
des Bundesbeauftragten für den Datenschutz in den Jahren 2003 und 2004 sowie
einen Ausblick auf anstehende wichtige Fragen.

Umfassend wird die Weiterentwicklung und Modernisierung des Datenschutz-
rechts begründet. Die Gefahren für das informationelle Selbstbestimmungsrecht
durch die immer weiter voranschreitenden technologischen Innovationen wer-
den verdeutlicht. Ebenso werden die zunehmende Bedeutung europäischer
Rechtsinstrumente und ihre Auswirkungen auf den Datenschutz aufgezeigt.

Zudem enthält die Unterrichtung wesentliche Feststellungen zur datenschutz-
rechtlichen Kontrolle von öffentlichen Stellen des Bundes.

B. Lösung
Kenntnisnahme der Unterrichtung und einstimmige Annahme der Ent-
schließung

C. Alternativen
Keine

D. Kosten
Keine
Beschlussempfehlung

Der Bundestag wolle beschließen, in Kenntnis der Unterrichtung auf Drucksache 15/5252 folgende Entschließung anzunehmen:


3. Der Deutsche Bundestag erwartet von der Bundesregierung, dass sie seine mehrfach erhobene Forderung aufgreift, den Arbeitnehmerdatenschutz gesetzlich zu regeln, und unverzüglich einen entsprechenden Gesetzentwurf vorlegt (20. TB, Nr. 2.5 und 10.1).

4. Der Deutsche Bundestag unterstützt die Bemühungen zur Schaffung eines europäischen Raums der Freiheit, der Sicherheit und des Rechts. Hierzu zählt auch die Schaffung eines hohen und harmonisierten Datenschutzstandards in der dritten Säule der EU. Ein gemeinsamer europaweiter Datenschutzstandard würde auch das Verfahren der grenzüberschreitenden Datenübermittlung vereinheitlichen und damit den Informationsaustausch zwischen den Polizei- und Sicherheitsbehörden erleichtern. Die Bundesregierung wird deshalb aufgefordert, sich auf der Basis des Rahmenbeschlusses über den Datenschutz in der dritten Säule der EU für eine zügige Verabschiedung entsprechender datenschutzrechtlicher Regelungen auf diesem Gebiet innerhalb der deutschen Ratspräsidentschaft einzusetzen (20. TB Nr. 3.3.4).


noch Anlage 4

Nicht erledigt
s. 22. TB Nr. 2.2 f.

Noch nicht erledigt, aber aufgegriffen im Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften (Bundesratsdrucksache 4/09)
s. 22. TB Nr. 2.4

Nicht erledigt
s. 22. TB Nr. 11.1

Erledigt
s. 22. TB Nr. 13.3.1

Erledigt
s. 22. TB Nr. 16.21


10. Der Bundestag erinnert an die Zusage des Bundesministeriums der Finanzen, den Betroffenen auch gegenüber der Steuerverwaltung einen Anspruch auf Auskunft zu den über sie gespeicherten Daten einzureißen. Der Stellungnahme der Bundesregierung ist zu entnehmen, dass dieser Auskunftsanspruch deswegen noch nicht in ein Gesetzgebungsvorhaben eingebracht worden ist, weil „zuvor die personellen, organisatorischen und haushaltswirtschaftlichen Auswirkungen“ geprüft werden müssten. Der Deutsche Bundestag fordert die Bundesregierung auf, diese Prüfungen nunmehr zeitnah abzuschließen und die gesetzliche Regelung eines Auskunftsanspruchs in der AO in die Wege zu leiten (20. TB Nr. 8.1).


Noch nicht erledigt, da sich das BMF trotz BVerfG-Beschlusses und der BT-Entschließung zum 20. TB weiterhin weigert, Auskunftsrechte der Betroffenen anzuerkennen

s. 22. TB Nr. 9.5

Erledigt

§ 93 Abs. 8 AO alte Fassung wurde durch § 93 Abs. 8 - 10 AO neue Fassung ersetzt. Aus § 93 Abs. 8 AO ergeben sich mittelbar die Behörden, die zum Kontenabrf berechtigt sind, die Abrufvoraussetzungen und die Zweckbestimmungen.

s. 22. TB Nr. 9.4

Deutscher Bundestag
16. Wahlperiode

Beschlussempfehlung und Bericht
des Innenausschusses (4. Ausschuss)

zu der Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
– Drucksache 16/4950 –

Tätigkeitsbericht 2005 und 2006 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
– 21. Tätigkeitsbericht –

A. Problem

B. Lösung
Kenntnisnahme der Unterrichtung und einstimmige Annahme einer Entschließung

C. Alternativen
Keine

D. Kosten
Keine
Beschlussempfehlung

Der Bundestag wolle beschließen, in Kenntnis der Unterrichtung auf Drucksache 16/4950 folgende Entschließung anzunehmen:


Dieses Projekt muss jetzt zügig vorangebracht werden, damit ein Datenschutzauditgesetz noch in dieser Legislaturperiode verabschiedet werden kann (21. TB, Nr. 2.4).

2. Der Abstand zwischen den geltenden datenschutzrechtlichen Bestimmungen und der rasanten technologischen Entwicklung mit ihren Folgen in allen Lebensbereichen wird immer größer. Das vom Deutschen Bundestag geforderte moderne, leichtverständliche und übersichtliche Datenschutzrecht wäre nicht nur ein wirtschaftlicher Standortvorteil, sondern könnte auch einen wertvollen Beitrag zur Entbürokratisierung leisten (21. TB, Nr. 2.1).

3. Der Deutsche Bundestag beobachtet sorgfältig die Entwicklung von Informations- und Kommunikationstechnologien, die neben Vorteilen für das tägliche Leben auch neue Risiken wie z. B. Identitätsdiebstahl, diskriminierende Profilerstellung oder Betrugsdelikte mit sich bringen.

Die Bundesregierung wird aufgefordert, dafür Sorge zu tragen, dass datenschutzfreundliche Technologien weiter entwickelt, verbreitet und verwendet werden, um den Schutz der Privatsphäre und den Datenschutz zu verbessern.

4. Nachdem auf europäischer Ebene eine Initiative zum Arbeitnehmerdatenschutz nicht mehr zu erwarten ist, weist der Deutsche Bundestag die Bundesregierung noch einmal nachdrücklich auf seine mehrfach erhobene Forderung hin, schnellstmöglich einen Gesetzentwurf zum Arbeitnehmerdatenschutz vorzulegen (21. TB, Nr. 2.7).


Dieser Aufforderung ist die Bundesregierung noch immer nicht nachgekommen. Der Deutsche Bundestag fordert die Bundesregierung deshalb erneut auf, den Auskunftsanspruch des Betroffen auch in der Steuerverwaltung sicherzustellen.

6. Der Deutsche Bundestag fordert die Bundesregierung auf, die Bürgerinnen und Bürger besser vor den Gefahren des Missbrauchs biometrische Systeme zu schützen. Bei der Entwicklung von Biometrieanwendungen muss ein hoher Datenschutzstandard gewährleistet sein, so dass der Datenschutz der Bürgerinnen und Bürger sichergestellt ist und Missbrauchsmöglichkeiten ausgeschlossen sind.

7. Der Deutsche Bundestag teilt die Auffassung der Bundesregierung, dass das Bundesdatenschutzgesetz auch für Rechtsanwälte gilt. Er begrüßt, dass die Bundesregierung prüft, welche gesetzlichen Regelungen sich im Zusammenhang mit der Verarbeitung mandatsbezogener Daten durch Rechtsanwälte empfehlen, um eine wirksame Datenschutzkontrolle zu gewährleisten, ohne dass das besonders geschützte Vertrauensverhältnis zwischen Rechtsanwalt und Mandant in unzulässiger Weise beeinträchtigt wird.

Resolution über den dringenden Bedarf an globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenschutzzwecken herangezogen werden

Antragsteller: Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit (Deutschland)
Unterstützt von: Österreichische Datenschutzkommission (Österreich)
Office of the Privacy Commissioner of Canada (Kanada)
Office of the Information and Privacy Commissioner of British Columbia
Office of the Information and Privacy Commissioner of Ontario
European Data Protection Supervisor (Europäische Gemeinschaft)
La Commission Nationale de l'Informatique et des Libertés (Frankreich)
Landesbeauftragte für Datenschutz und die Informationsfreiheit Nordrhein-Westfalen (Deutschland – Regional)
Garante per la protezione dei dati personali (Italien)
College Bescherming Persoonsgegevens (Niederlande)
Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Rumänien)
Agencia de Protección de Datos (Spanien)
Information Commissioner (Vereinigte Königreich)

Die Konferenz beruft sich auf
– das 2002 auf der 24. Internationalen Konferenz in Cardiff angenommene Kommuniqué;
– die 2003 auf der 25. Internationalen Konferenz in Sydney angenommene Resolution über die Übertragung von Passagierdaten;

Die Konferenz vermerkt, dass
– Regierungsstellen zunehmend den Zugriff zu Passagierdaten suchen, die im Kampf gegen den Terrorismus, gegen illegale Einwanderung und andere Verbrechen verwendet werden sollen, ohne dass genügend Rücksicht auf Persönlichkeits- und die Menschenrechte der Passagiere genommen wird;
– manche Passagierdaten dazu benutzt werden können, Folgerungen über Religionszugehörigkeit, Ethnie und andere äußerst heikle Zusammenhänge zu ziehen,
– weltweit viele Regierungen ständig mehr Daten von Verkehrsträgern verlangen,
– Verkehrsträger die Passagierdaten aus kommerziellen Gründen erfassen und dann aufgefordert werden, sie für Justizvollzugszwecke zur Verfügung zu stellen,
– Verkehrsträger zunehmend viele verschiedene Forde rungen zur Übergabe von Daten erfüllen müssen und sich an viele verschiedene Datenübertragungssysteme halten müssen, wodurch unter den Verkehrsträgern wie auch unter den Passagieren Ungewissheit über ihre Rechte und Pflichten entsteht, wodurch die Passagiere nur schwer verstehen, wie ihre Daten genutzt werden, und wodurch auch das Risiko entsteht, dass die Verkehrsträger die Daten unsachgemäß übertragen,
– diese vielen verschiedenen Forderungen und Systeme sowohl für die Verkehrsträger als auch für die Passagiere mit Kosten verbunden sind,
– juristische und technische Übereinstimmung erforderlich ist, damit die Verkehrsträger diese Forderungen erfüllen können,
– manche Verkehrsträger immer noch nicht ihrer Pflicht nachkommen, Passagiere über die Verwendung und Offenlegung ihrer Daten zu unterrichten,
– andere globale Abmachungen zur Erleichterung des internationalen Flugverkehrs getroffen worden sind, und dass dringender Bedarf besteht, globale Lösungen zu treffen, die den internationalen Reiseverkehr erleichtern und dabei das Recht der Passagiere auf Persönlichkeitsschutz respektieren.

Die Konferenz bestätigt erneut, dass
– Datenschutz und Schutz der Privatsphäre – wie in Artikel 12 der Allgemeinen Deklaration der Menschenrechte und in anderen Rechtsinstrumenten verankert – Privatpersonen und ihre persönlichen Daten schützen und zusammen mit anderen Rechten in allen Ersuchen zur Übertragung und Nutzung von Passagierdaten für Justizvollzugszwecke berücksichtigt werden müssen,
die Verarbeitung von Passagierdaten in einem Rahmen stattfinden sollte, der die anerkannten Datenschutzgrundsätze und -standards berücksichtigt,
in allen Ersuchen staatlicher Behörden für die Nutzung von Passagierdaten Folgendes nachgewiesen werden sollte:

- sie sind nachweisbar notwendig, um ein spezifisches Problem anzusprechen,
- sie sind nachweisbar mit Wahrscheinlichkeit geeignet, das Problem anzusprechen,
- sie entsprechen proportional ihrem Sicherheitswert, und sie greifen nachweisbar weniger in die Privatsphäre ein als alternative Optionen, sowie
- um festzustellen, ob die Maßnahmen noch erforderlich sind,

- die Notwendigkeit, unter allen Umständen die Privatsphäre zu schützen, nicht nur für globale Datenschutzkreise, sondern auch für alle eine grundsätzliche Aufgabe bleibt, die um die Wahrung der fundamentalen Rechte und Freiheiten besorgt sind, und
- wenn Regierungsstellen sich nicht bemühen, die Datenschutzbelange richtig zu wägen, die echte Gefahr besteht, dass diese Stellen beginnen könnten, die fundamentalen Rechte und Freiheiten selbst, die sie schließlich schützen wollen, zu unternimieren.

Im Bestreben nach globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden, ruft die Konferenz dazu auf,

dass internationale Organisationen (wie z.B. IATA und ICAO), Regierungsstellen und Verkehrsträger mit den Beauftragten für den Datenschutz und für die Privatsphäre zusammenarbeiten, um verbindliche globale Lösungen mit angemessenen Datenschutzsicherheiten einzuführen,

dass Regierungsstellen gewährleisten, dass alle Ersuche für die Nutzung von Passagierdaten

- nachweisbar notwendig sind, um ein spezifisches Problem anzusprechen,
- nachweisbar mit Wahrscheinlichkeit geeignet sind, das Problem anzusprechen;

- ihrem Sicherheitswert proportional entsprechen, und

- nachweisbar weniger in die Privatsphäre eingreifen als alternative Optionen, sowie dass all solche Ersuche regelmäßig überprüft werden sollten, um festzustellen, ob die Maßnahmen noch erforderlich sind,

- dass alle Passagierdaten nutzenden staatlichen Programme für Datenminimalisierung sowie für die ausdrückliche Beschränkung der Nutzung, Offenlegung und Einbehaltung der Daten auf die entsprechenden Programmzwecke sowie für die Richtigkeit der Daten, für das Recht auf Zugriff zu den Daten, für die Korrigierung der Daten und für eine unabhängige Überprüfung sorgen sollten,

- dass alle Lösungen die juristischen, technischen, finanziellen und wirtschaftlichen Belange der Verkehrsträger und der Behörden berücksichtigen müssen,

- dass Regierungsstellen offen und transparent die Zwecke, zu denen die Daten gesammelt und genutzt werden, angeben, und sicher stellen, dass alle Passagiere – ungeachtet ihrer Nationalität oder ihres Herkunftslandes – Zugang zu ihren persönlichen Informationen sowie zu einem angemessenen Rechtshilfemechanismus haben,

- dass Verkehrsträger ihre Passagiere über die Nutzung und Offenlegung ihrer Daten durch Regierungsstellen und Justizvollzugsbehörden, über Flugverbotslisten und ähnliche Überwachungslisten sowie über die Verfügbarkeit von Rechtshilfemaßnahmen im Zusammenhang mit Passagierdaten und damit zusammenhängenden persönlichen Informationen ausreichend unterrichten, und

- dass die Beauftragten für den Datenschutz und den Schutz der Privatsphäre weiterhin zusammenarbeiten, um sachgemäße Datenschutzmaßnahmen zu gewährleisten und auf verbindliche globale Lösungen zu drängen.

Erläuternder Hinweis

Die Regierungen verschiedener Länder haben zunehmend versucht, Passagierdaten als Waffe im Kampf gegen Terrorismus, transnationale Kriminalität und andere Verbrechen zu nutzen. Dadurch sind in Bezug auf die geforderten Datenelemente, die Verwendung der Daten und die Stufe der Sicherheitsmaßnahmen Differenzen aufgetreten.

Das Wesen des internationalen Reiseverkehrs fordert einen globalen Ansatz, und es ist eine globale Lösung dringend erforderlich, um eine angemessene Sicherheitsstufe zu erlangen und das Vertrauen der Passagiere zu gewinnen, während proportionale Maßnahmen unternommen werden, die den notwendigen Datenschutz und den Schutz der Privatsphäre beinhalten. Während Bedenken über den Datenschutz und den Schutz der Privatsphäre die vorrangigen Themen darstellen, die bei jeder globalen Lösung zu berücksichtigen sind, bietet sich auch Gelegenheit, andere juristische, technische, finanzielle und wirtschaftliche Fragen von Fluggesellschaften und Passagieren in Betracht zu ziehen.

Globale Standards können die Fairness, Übereinstimmung, juristische Gewissheit und Sicherheit für Passagiere und Verkehrsträger gewährleisten. Es ist klar, dass Verkehrsträger, Justizvollzugsbehörden, internationale Orga-
nisationen, zivilgesellschaftliche Gruppen und Datenschutzexperten an der globalen Lösung beteiligt sein müssen. Das Engagement der Datenschutzbeauftragten ist unentbehrlich, wenn Fortschritte erzielt werden sollen. Sie müssen die Führung übernehmen und auf einer solchen Lösung bestehen.
Antragsteller: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland
Unterstützt durch:
Commission Nationale de l’Informatique et des Libertés (CNIL), Frankreich;
Bundesbeauftragter für Datenschutz und Informationsfreiheit, Deutschland;
Garante per la protezione dei dati personali, Italien;
College Bescherming Persoonsgegevens, Niederlande;
Privacy Commissioner, Neuseeland;
Eidgenössischer Datenschutz und Öffentlichkeitsbeauftragter (EDÖB), Schweiz

Entschließung


2 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208436491

Empfehlungen

In Anbetracht der besonderen Natur der Dienste und der kurz- und langfristigen Gefahren für die Privatsphäre des Einzelnen richtet die Konferenz folgende Empfehlungen an Nutzer und Anbieter sozialer Netzwerkdiensie:

Nutzer sozialer Netzwerkdiensie

Organisationen, denen am Wohl der Nutzer sozialer Netzwerke gelegen ist – einschließlich Diensteanbieter, Regierungen und Datenschutzbehörden – sollten mithelfen, die Nutzer über den Schutz ihrer personenbezogenen Daten aufzuklären und die folgende Botschaften zu vermitteln.

1. Veröffentlichung von Daten

Nutzer sozialer Netzwerkdiensie sollten sich sorgfältig überlegen, welche persönlichen Daten sie – wenn überhaupt – in einem sozialen Netzwerkprofi publizieren. Sie sollten bedenken, dass sie zu einem späteren Zeitpunkt mit einer Information oder mit Bildern konfrontiert werden könnten, z. B. wenn sie sich um eine Arbeitsstelle bewerben.


2. Die Privatsphäre Anderer

Nutzer sollten auch die Privatsphäre Anderer achten. Sie sollten besonders vorsichtig sein bei der Veröffentlichung personenbezogener Daten Anderer (einschließlich Bildern, oder sogar mit Zusatzinformationen versehenen Bildern) ohne die Einwilligung der betreffenden Personen.

Anbieter sozialer Netzwerkdiensie

Anbieter sozialer Netzwerkdiensie tragen eine besondere Verantwortung dafür, die Belange von Personen, die soziale Netzwerke nutzen, zu beachten und zu wahren. Sie sollten nicht nur die Regelungen des Datenschutzrechts einhalten, sondern auch die folgenden Empfehlungen umsetzen.

1. Datenschutzvorschriften und -standards

Anbieter, die in verschiedenen Ländern oder sogar weltweit tätig sind, sollten die Datenschutzstandards der Länder einhalten, in denen sie ihre Dienste betreiben. Zu diesem Zweck sollten die Anbieter Datenschutzbehörden konsultieren, wenn und soweit dies notwendig ist.

2. Aufklärung der Nutzer


3. Nutzerkontrolle


4. Datenschutzfreundliche Standardeinstellungen

Darüber hinaus sollten Anbieter datenschutzfreundliche Standardeinstellungen für Nutzerprofildateninformationen anbieten. Standardeinstellungen spielen eine Schlüsselrolle beim Schutz des Privatsphäre der Nutzer: Es ist bekannt, dass lediglich eine Minderheit von Nutzern, die sich bei einem Dienst anmelden, irgendwelche Änderungen daran vornimmt. Diese Einstellungen müssen bei einem sozialen Netzwerkdiensie, der sich an Minderjährige wendet, besonders restriktiv sein.

5. Sicherheit

Anbieter sollten die Sicherheit ihrer Informationssysteme weiter verbessern und aufrechterhalten und die Nutzer ge-
gen betrügerische Zugriffe auf ihre Profile schützen, indem sie für die Konzeption, die Entwicklung und den Betrieb ihrer Anwendungen anerkannte Methoden einschließlich unabhängiger Auditing und unabhängiger Zertifizierung verwenden.

6. Auskunftsrechte

Anbieter sollten Personen (gleichgültig ob Mitglieder des sozialen Netzwerkdienstes oder nicht) ein Recht auf Auskunft zu ihren personenbezogenen Daten gewähren und erforderlichenfalls diese Daten berichten.

7. Löschung von Nutzerprofilen

Anbieter sollten den Nutzern die Möglichkeit geben, ihre Mitgliedschaft auf einfache Weise zu beenden und ihre Profile sowie alle Inhalte oder Informationen, die sie in dem sozialen Netzwerk publiziert haben, zu löschen.

8. Pseudonyme Nutzung des Dienstes

Anbieter sollten als Option die Möglichkeit der Einrichtung und Verwendung pseudonymer Profile anbieten und zur Nutzung dieser Option ermutigen.

9. Zugriff durch Drittpersonen

Anbieter sollten wirksame Maßnahmen ergreifen, um das Durchsuchen und/oder massenweise Herunterladen (oder „bulk harvesting“) von Profildaten durch Dritte zu verhindern.

10. Indexierbarkeit der Nutzerprofile

Entschließung zum Schutz der Privatsphäre von Kindern im Internet

Antragstellerin: Die Datenschutzbeauftragte von Kanada
Unterstützt durchs : Datenschutzbeauftragter, Neuseeland
La Commission Nationale de l’Informatique et des Libertés (Frankreich)
Datenschutzbeauftragter, Irland
Beauftragter für den Datenschutz und Informationsfreiheit, Berlin


Dabei werden die Jugendlichen auch mit den Schwierigkeiten und Herausforderungen bezüglich des Schutzes ihrer persönlichen Daten im Internet konfrontiert. Das Fehlen einer Regelung bei zahlreichen Internet-Diensten macht die Sache schwierig. Viele der bei Jugendlichen beliebtesten Websites sammeln große Mengen personenbezogener Daten für Verkaufs- und Marketingzwecke.

Mit steigender Anzahl der im Internet angebotenen Anwendungen und Technologien wird die Menge der gesammelten und aufbewahrten personenbezogenen Daten immer größer. Heute sind sich die Jugendlichen oft nicht darüber bewusst, dass ihre Auskünfte, ihre Gewohnheiten und ihre Verhaltensweisen im Internet überwacht werden. Untersuchungen zeigen, dass die Jugendlichen (wie auch zahlreiche Erwachsene) nur selten die Geheimhaltungsklärungen der von ihnen besuchten Websites lesen, was nicht überrascht, denn die Vertraulichkeitsklärungen zahlreicher Websites sind in einer technischen oder juristischen Fachsprache abgefasst, die für die meisten Leser schwer verständlich ist.

Wenn auch manche Jugendliche die mit ihren Online-Aktivitäten verbundenen Gefahren erkennen, so verfügen sie doch nicht über die Erfahrung, die technischen Kenntnisse oder die nötigen Instrumente, um diese Gefahren zu mindern. Oft kennen sie ihre gesetzlichen Rechte nicht.

Vor fast 20 Jahren hat die Generalversammlung der Ver einen Nationen 1989 ein Übereinkommen über die Rechte des Kindes verabschiedet. In diesem heißt es, dass die Staaten die Rechte des Kindes achten und schützen müssen, einschließlich ihres Rechtes auf den Schutz ihrer Privatsphäre.

Seit dieser Zeit bereiteten den Datenschutzbeauftragten die Verletzungen der Privatsphäre von Kindern im Internet immer mehr Sorgen.

In der am 20. Februar 2008 vom Ministerrat des Europarat angenommenen Erklärung zum Schutz der Würde, Sicherheit und der Privatsphäre von Kindern im Internet zeigt sich dieser von der Notwendigkeit überzeugt, Kinder über die lange Speicherdauer und über die Risiken der von ihnen ins Internet eingestellten Inhalte aufzuklären.

Er erklärte darüber hinaus, dass, anders als bei der Strafverfolgung, keine fortbestehenden oder dauerhaft zugänglichen Aufzeichnungen über die von Kindern ins Internet eingestellten Inhalte existieren sollten, die deren Würde, Sicherheit und Privatsphäre angreifen oder ihnen auf andere Art und Weise jetzt oder zu einem späteren Zeitpunkt ihres Lebens schaden können.

Die Datenschutzbeauftragten haben zugleich erkannt, dass ein auf Erziehung ausgerichteter Ansatz, verbunden mit einer Regelung des Datenschutzes, eine der wirksamsten Methoden zur Bewältigung dieses Problems darstellt. So haben mehrere Länder innovative, auf Erziehung angelegte Konzepte umgesetzt, um der Herausforderung zu begegnen, die der Schutz der Privatsphäre von Kindern im Internet darstellt.

Kinder und Jugendliche haben ein Recht darauf, sich online sicher bewegen und positive Erfahrungen machen zu können, bei denen sie die Absichten der Personen, mit denen sie interagieren, kennen und verstehen.

Die auf der 30. internationalen Konferenz versammelten Beauftragten für den Datenschutz und für die Privatsphäre haben beschlossen:

– die Erarbeitung von Ansätzen zu fördern, die auf Erziehung angelegt sind, um die Lage in Bezug auf den Schutz der Privatsphäre im Internet auf nationaler wie internationaler Ebene zu verbessern;
– bemüht zu sein, dafür zu sorgen, dass Kinder und Jugendliche in der ganzen Welt Zugang zu einem sicheren Online-Umfeld haben, das ihre Privatsphäre respektiert;
– mit Partnern und Akteuren im eigenen Land und im Ausland zusammenzuarbeiten, in der Erkenntnis, dass die Zusammenarbeit mit den Fachleuten, die das tägliche Leben der Kinder beeinflussen, von entscheidender Bedeutung ist;
– miteinander zu arbeiten, um beispielhafte Praktiken auszutauschen und Aktivitäten zur Erziehung der Öffentlichkeit durchzuführen, um Kinder und Jugendli-
noch Anlage 8

die stärker zu sensibilisieren hinsichtlich der Gefahren in Bezug auf den Schutz ihrer Privatsphäre, die mit ihren Online-Aktivitäten verbunden sind, und bezüglich der sich ihnen bietenden Möglichkeiten einer aufgeklärten Wahl, um ihre persönlichen Informationen zu kontrollieren;

– bei Erziehenden die Einsicht zu fördern, dass die Sensibilisierung für den Schutz der Privatsphäre einen wesentlichen Aspekt der Kindererziehung darstellt und in ihr Unterrichtsprogramm aufgenommen werden muss;

– zu fordern, dass die Behörden Gesetze erlassen, die die Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern einschränken, einschließlich geeigneter Bestimmungen für den Fall von Verstößen;

– bei Online-Werbung für Kinder oder verhaltensbezogener Werbung geeignete Einschränkungen bei der Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern zu fordern;

– die Betreiber von Websites für Kinder anzuhalten, ihr soziales Bewusstsein unter Beweis zu stellen, indem sie Vertraulichkeitserklärungen und Nutzungsvereinbarungen einführen, die klar, einfach und verständlich sind und indem sie die Nutzer über die Gefahren für den Schutz der Privatsphäre und die Sicherheit sowie über die ihnen auf der Website gebotenen Wahlmöglichkeiten aufklären.
Erklärung der Europäischen Datenschutzkonferenz von Zypern, angenommen am 11. Mai 2007

Im Rat der Europäischen Union ist ein Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Gegenstand von Beratungen.

Die Schaffung eines harmonisierten und hohen Standards für den Datenschutz bei polizeilichen und justiziellen Maßnahmen in der Union ist in der Tat ein entscheidender Bestandteil der Achtung und des Schutzes von Grundrechten, wie es auf dem Schutz personenbezogener Daten, bei der Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts.


Diese Initiativen zeigen deutlich, dass die Verpflichtung der Union zur Hilfe beim Kampf gegen schwere Straftaten und Terrorismus nicht auf die Schaffung der Bedingungen für den Informationsaustausch zwischen den Mitgliedstaaten beschränkt ist; klar erkennbar haben die Initiativen auch Auswirkungen auf die Datenverarbeitung auf nationaler Ebene, die jedem möglichen Austausch vorausgeht. Es ist klar, dass jede Entwicklung auf diesem Gebiet abgewogen werden muss mit angemessenen und harmonisierten Datenschutzrechten und -verpflichtungen, wobei das gegenseitige Vertrauen in diese ein entscheidender Bestandteil ist.

Innerhalb der Europäischen Union unterscheidet sich die Datenschutz-Gesetzgebung für Maßnahmen der Strafverfolgung sowohl der Natur als auch der Sache nach. Sie gewährleistet somit sicherlich keinen harmonisierten Ansatz zum Datenschutz für Strafverfolgungs-Informationen, für die Rechte des Betroffenen sowie für eine effektive unabhängige Kontrolle.

Im Hinblick auf den zunehmenden Rückgriff auf die Verfügbarkeit („availability“) von Informationen als Konzept zur Verbesserung des Kampfes gegen schwere Straftaten, sowohl auf nationaler Ebene wie zwischen den Mitgliedstaaten, fällt das Fehlen eines harmonisierten und hohen Standards für den Datenschutz in der Union zu einer Situation, in der das Grundrecht auf den Schutz personenbezogener Daten nicht mehr ausreichend gewährleistet wird.


Die Europäische Datenschutzkonferenz ist sich über die Grundsatz-Diskussion im Rat über den Anwendungsbe- reich des vorgeschlagenen Rahmenbeschlusses bewusst: sollte er nur auf Daten anwendbar sein, die zwischen Mitgliedstaaten ausgetauscht werden oder auf jegliche Verarbei- tung durch Polizei- und Justizbehörden?

Die Europäische Datenschutzkonferenz weist wiederholt darauf hin, dass Initiativen der Union Auswirkungen auf nationaler Ebene haben und darauf, dass eine Begrenzung des Anwendungsbereiches auf Daten, die zwischen den Mitgliedstaaten ausgetauscht werden oder werden könnten, das Risiko besonderer Unsicherheiten und Unwägbarkeiten über den Anwendungsbereich des vorgeschlagenen Rahmenbeschlusses mit sich bringen würde. Sie betont, dass nur ein umfassender Anwendungsbereich unter Einschluss aller Arten der Verarbeitung personenbezogener Daten den notwendigen Schutz der Individuen gewährleisten kann.


Während der Entwurf einige Verbesserungen im Hinblick auf die Erreichung eines harmonisierten Rahmens für die Verarbeitung gebracht hat, ist er bislang unbefriedigend bei den Vorkehrungen zur Gewährleistung des Schutzes der Privatsphäre der Bürger. Dies muss besonders gelten, wenn man die bereits bestehende europäische Gesetzge- bung zum Datenschutz berücksichtigt, insbesondere den rechtlichen Rahmen, der von den nationalen Gesetzgebern bei der Umsetzung der Richtlinie 95/46/EG geschaffen wurde und der ebenfalls auf die Verarbeitung personenbezogener Daten in dem fraglichen Bereich anwendbar ist. Darüber hinaus wiederholt die Europäische Datenschutzkonferenz, dass es notwendig ist, die auf nationaler Ebene bestehenden Schutzvorkehrungen zum Datenschutz zu er- halten, indem ein bindendes europäisches Instrumentarium verabschiedet wird.

Mit dem Ziel einer tatsächlichen Verbesserung beim Da- tenschutz in der dritten Säule unterstreicht die Europäische Datenschutzkonferenz die folgenden Grundsätze,
noch Anlage 9
die bei dem wichtigen Gesetzgebungsakt Rahmenbeschluss zu beachten sind:


- Kategorien von Betroffenen: Es ist ein Erfordernis des Verhältnismäßigkeitsgrundsatzes, Unterscheidungen zwischen den verschiedenen Kategorien von Personen wieder einzuführen, die von der Verarbeitung für Polizei und Strafverfolgung betroffen sind.


Die Europäische Datenschutzkonferenz ruft den Rat daher dazu auf, sich mehr Zeit für die Verhandlungen zur Entwicklung eines Rahmenbeschlusses zu nehmen, der einen hohen Datenschutz-Standard bietet.

Die Europäische Datenschutzkonferenz ist bereit, weiter zum Verfahren der Verabschiedung eines solchen Rahmenbeschlusses beizutragen und schlägt eine Anhörung der Arbeitsgruppe des Rates vor, um ihre Standpunkte darzulegen.
Die Europäische Union wird in Kürze über verschiedene neue Initiativen zur verbesserten Kontrolle von Reisenden in die Europäische Union und aus der Europäischen Union, diskutieren. Drei von der Kommission vor kurzem verabschiedete Mitteilungen⁴ haben zum Ziel, eine solche Diskussion über die nächsten Schritte zum Border Management, sowie über die Schaffung eines Europäischen Grenzüberwachungssystems und über die Bewertung von Frontex in Gang zu bringen.


Obwohl ein effizientes Border Management für den Schutz der Union gegen mögliche Bedrohungen notwendig ist, so darf dies niemals in unverhältnismäßiger Weise die Rechte und Freiheiten der Reisenden, und vor allem nicht deren Recht auf Privatsphäre verletzen. Die Überwachung der Reisenden muss wohlbegründet sein und darf nur in Ausnahmefällen gestattet werden, und dies auch nur für berechtigte und besondere Zwecke. Jede allgemeine Überwachung stellt nicht hinnehmbare Risiken für die Freiheit der Einzelnen dar.

Ein anderes Thema, das überdacht werden muss, ist das zu Grunde liegende Konzept, Reisenden zu misstrauen, in dem man ausgewählte „vertrauenswürdige“ Reisende von allen anderen Reisenden isoliert, und die letzteren sogar als potentielle Straftäter erachtet. Das wird eine Durchleuchtung vor und am Eingang beinhalten, so wie die Kontrolle der Grenzüberschreitungen und die automatische Verarbeitung spezieller Daten der Reisenden. Dieses Konzept trägt nicht gerade viel dazu bei, den „symbolischen Effekt, die EU als weltoffen darzustellen“⁵, zu verwirklichen, so wie es die Mitteilung der Kommission erwähnt, und es ist sogar fraglich, ob dies mit den Werten der Europäischen Union im Einklang steht.

Die Konferenz hat bereits die Mitglieder der Europäischen Union und die Kommission, den Rat und das Europäische Parlament dazu aufgerufen, zuerst einmal eine Evaluierung zu fertigen, ob die bereits bestehenden rechtlichen Maßnahmen effektiv umgesetzt und durchgeführt werden.⁶ Ein neuer Vorschlag sollte nur dann eingebracht werden und wenn klare Hinweise vorliegen, die solche Maßnahmen unterstützen.

Allerdings fand bis jetzt keine solche Bewertung über die Effektivität der Umsetzung der bestehenden rechtlichen Maßnahmen statt. Auch wurden keine verlässlichen Hinweise vorgelegt, die die Notwendigkeit neuer Systeme untermauern. Ebenso wenig wurden Beweise erbracht, die es erforderlich erscheinen lassen, die aktuellen Initiativen auf diesem Gebiet zu ergänzen.


Da dies anscheinend nicht der Fall ist, ruft die Konferenz die Europäische Union auf, die Notwendigkeit und Verhältnismäßigkeit weiterer Maßnahmen im Lichte der oben erwähnten Kommentare sorgfältig zu überdenken, und zwar vor allem in Bezug auf die in den Mitteilungen der Kommission vorgesehenen Vorschläge.

Sachregister
Als Fundstelle ist die Nummer des Abschnitts oder des Beitrages angegeben, in dem der Begriff verwendet wird.

A2LL 16.6
Abgabenordnung 9.4; 9.5
Abgeltungssteuer 9.2
Adresshandel 3.4.5
AG Versicherungswirtschaft 3.4.7
Agentur FRONTEX 13.3.7
Agentur für Arbeit 10.5.4
Akustische Wohnraumüberwachung 16.24
Allgemeine Gleichbehandlungsgesetz (AGG) 11.3
Anschriften- und Gebäuderegister (AGR) 5.5 ff.
Anti-Terror-Datei 4.2; 4.2.2 ff.
Anti-Terror-Datei-Gesetz 4.2.2
API Richtlinie 13.5 ff.
Arbeitgeber 4.8.3.2
Arbeitnehmerdatenschutz 11.1
Arbeitnehmerdatenschutzgesetz 1; 11.1
Arbeitsgemeinschaften (ARGE) 10.5.3
Arbeitsuchende 10.5.2
Arbeitsverwaltung 10.5 ff.
Artikel-29-Gruppe 3.4.1; 7.6; 13.2 ff.; 13.3; 13.3.7; 13.3.8
Atomgesetz 4.8.3; 4.8.3.1
Aufsichtsbehörden 15.6
Auftragsdatenverarbeitung 2.5; 2.6; 3.2.3
Ausbildung 15.10
Auskunftei 3.4.4
Auskunftsanspruch 1; 4.7.3.3; 9.5
Auskunftsersuchen 7.11
Auskunftsrecht 9.5
Auskunftsverlangen nach § 188 Satz 2 SGB VII 10.3.2
Ausländerrecht 16.1
Ausländerzentralregister 5.7; 13.3.4; 16.1
Auslandsvertretung 14.2
Auswärtiges Amt 4.2.3
Auswertedateien 4.2.4
amtomatisiertes Mitteilungs- und Auskunftsverfahren 4.6
BA-Internet-Plattform 16.7
Basic Access Control (BAC) 6.3.1
Behördenrufnummer 2.7
Behördlicher Datenschutzbeauftragter 3.2.2; 15.5
Beihilfe 11.2
Beihilferecht 11.2
Berufsanerkennungsrichtlinie 3.4.1
Berufsgeheimnis 2.6
Berufsgeheimnisträger 3.4.6
Berufsagenossenschaften 10.3.1
Berufssoldaten 14.1
Bewerbungsunterlagen 11.3
Binding Corporate Rules 13.2.3
Binnenmarktinformationssystem (Internal Market Information System – IMI) 3.4.1
biometrische Daten 6.3 ff.; 13.3.4
BKA 4.2.2; 4.2.2.1; 4.3.1; 4.3.2; 4.3.2.1; 4.3.2.3
BKA-Gesetz 4.3.1; 13.7
BND 4.2.3; 4.7.2; 4.7.3.1; 4.7.3.2; 4.7.3.3;
Bonitätsprüfung 3.2.5
Border Management 13.3.7; 13.8
Botschaft 14.2
Briefverkehr 3.3.1
Bundesagentur für Arbeit 7.5; 10.5.1; 16.6; 16.7
Bundesamt für Güterverkehr 8.2; 12.1
Bundesamt für Justiz 8.2; 4.6
Bundesamt für Migration und Flüchtlinge 4.2.3; 16.3
Bundesamt für Sicherheit in der Informationstechnik 8.4
Bundesamt für Verfassungsschutz 4.2.3; 4.7.1
Bundesanzeiger 3.4.3
Bundesarchivgesetz 5.6
Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) 5.8
Bundeskriminalamt 4.2.2.2; 4.2.3; 4.2.4; 7.10; 13.7; 16.21
Bundesmeldegesetz 5.2; 6.5
Bundesmelderegister 5.2; 6.5
Bundesministerium der Verteidigung 16.10; 16.11
Bundesnotarkammer 16.8
Bundespolizei 4.2.3; 4.4; 6.4; 13.7
Bundesverwaltungsamt 4.2.1; 13.3.5
Bundeswehr 14.1; 16.11
Bundeszentralamt für Steuern 9.1 bis 9.3
Bundeszentralregister 4.6
Bürgerportal 6.6
Bürgerportalgesetz 6.6
Bürokratie 2.8
Bürokratiekosten 2.8

Call-Center 1; 3.2.3; 10.2.1; 10.2.1
Call-Me-Funktion 7.6
Charta der Grundrechte 13.1
Code of Conduct 3.4.7
Computer 8.3

daktyloskopische Daten 13.3.2
Datenaggregate 5.3
Datenerhebung (durch den Bundesnachrichtendienst) 4.7.3.1
Datenhandel 3.4.5
Datenlöschung 8.3
Datensammlung 3.1
Datenschutzaudit 2.4
Datenschutzaufsicht 10.5.3; 15.6
Datenschutzkonferenz 13.8; 13.9; 15.1
Datenschutzkontrollbehörden, europäische 13.3
Datenschutzskandal 3.1
Datenträger 8.2
Datenübermittlung 13.7
Datenverarbeitung 3.4.5; 4.7.3.1
De-Mail 6.6
De-Safe 6.6
Deutsch-amerikanisches Regierungsabkommen 13.4
Deutsche Post Adress GmbH 3.3.2
Deutsche Post Direkt GmbH 3.3.2
Deutsche Telekom AG 1; 3.2.2; 3.2.4
Deutscher Bundestag 16.9
Dienstleistungen 3.4.1
Dienststelle BfDI 15.11

DNA 13.3.2
Dokumentationspflicht 13.7
Dopingbekämpfung 5.9
Dritte Säule 13.8
Düsseldorfer Kreis 3.4.7; 15.6
easyPass 6.4
E-Bundesanzeiger 3.4.3
E-Call 16.18
Einheitlichen Ansprechpartner 3.4.1
Einlader- und Warndatei 5.7
Einwilligung 4.8.3.2
Einwilligungs- und Schweigepflichtentbindungserklärung 3.4.7
Elektronische Fallakte 6.1.1.2
Elektronische Gesundheitsakte 6.1.1.1
Elektronische Gesundheitskarte 6.1
Elektronische Identität 6
Elektronische Patientenakte 6.1
Elektronischer Entgeltnachweis (ELENA-Verfahrensgesetz) 6.2
Elektronischer Pass/E-Pass 6.3.1
Elektronisches Unternehmensregister 3.4.3
ElsterLohn II 9.3
Energieausweis 3.4.2
Energieeinspargesetz 3.4.2
Energieeinsparverordnung 3.4.2
Entlassungsberichte (in der medizinischen Rehabilitation) 10.4; 16.13
EPOS 2.0 16.14
Erfahrungsaustausch, datenschutzrechtlicher 15.5; 15.6
Erhebungs- und Leistungssystem A2LL 16.6
EU-Außengrenzen 13.3.7
Europadoc 13.3.8
EUROJUST 13.3
Europäischer Datenschutzbeauftragte 3.4.1; 13.3.8
Europäische Datenschutzkonferenz 13.8
Europäische Dienstleistungsrichtlinie 3.4.1
Europäische Menschenrechtskonvention 13.1
Europäisches Grenzkontrollsystem (EUROSUR) 13.3.7
Europäischer Datenschutztag 15.2
Europäisches Visa-Informationssystem 16.2
EUROPOL 13.3; 13.3.3; 13.3.5; 13.3.8
EUROPOL-Informationssystem 13.3.8
EUROPOL-Übereinkommen 13.3.3
Event Data Recorder 16.18
Extended Access Control (EAC) 6.3.1

Festplatte 8.3
Filter 8.4
Finanzamt 9.4
Finanzkontrolle Schwarzarbeit 4.2.3; 16.5
Fingerabdruckdatenbank des FBI (AFIS) 6.3.1
Fluggastdaten (PNR-Daten) 13.5 ff.
Flugmedizinische Unterlagen 16.17
Flugpassagierdaten 13.5 ff.
Forschungsdatenzentren 16.19
Foto-Fahndung 6.3; 8.1
Führungszeugnis 4.6
Funkchip 6.7
Future Group 13.3

GAnGes 6.4
Geheimschutzbeauftragter 4.8.2
Geldwäschebekämpfung 16.22
Geldwäschereichlinie 16.22
Gemeinsames Analyse- und Strategiezentrum Illegale Migration (GASIM) 4.2; 4.2.3
Gemeinsame Kontrollinstanz von EUROPOL 13.3.3
Gemeinsame-Dateien-Gesetz 4.2
Gemeinsames Terrorismusabwehrzentrum – GTAZ 4.2
Genanalysen 10.1
Gendiagnostikgesetz 10.1
Generalebundesanwartschaft 4.5
Geoinformationen 7.1; 7.2
Geomarketing 7.1
Geo-Scoring 7.1
Gesetzliche Krankenkassen 10.2 ff.; 16.13
Gesetzliche Rentenversicherung 10.4
Gesetzliche Unfallversicherung 10.3 ff.
Gesundheitsdaten 10.2.3; 10.5.4; 14.1
Gesundheitsreform 10.2.1

Gewalttäter Sport 4.3.2.3
Google 7.2
GPS 7.8
Grenzkontrollen 6.4; 13.3.7; 13.5.4
Grenzüberschreitende Datenschutzkontrolle 13.3.8
Grenzüberschreitende Zusammenarbeit 13.3.2
Grenzverwaltung 13.3.7
Großveranstaltungen 4.8.3.2
Gutachterregelung 10.3.1

Haager Programm 13.3
Handelsregister 3.4.3
Handy 7.7
HERKULES 16.10
Hinweis- und Informationssystem (HIS) 3.4.7
Hinweispflicht 2.8
Homepage-Überwachung 7.10
Hooligan-Datei 4.3.2.3

Identitätsmanagement 6.; 6.5
IMI 3.4.1
Informationsaustausch 13.3.6
Informationsgesellschaft 3.1
Informationstechnologie 8
INPOL 4.3.2 ff.; 13.3.4
INPOL-Verbunddatei „Gewalttäter Sport“ 4.3.2.3
Institut für Wehrmedizinialstatistik und Berichtswesen der Bundeswehr 14.1
Internationale Datenschutzkonferenz 13.1; 13.9; 15.7
Internet 6.; 6.1.1; 7 ff.
Internet-Angebot 15.8
Internet-Tauschbörsen 7.4
IP-Adressen 7.11
IPR-Enforcement-Richtlinie 7.4
IT-Sicherheit 6.6; 8.4
IT-Systeme 4.1; 4.1.2; 4.3.1; 8
Jahressteuergesetz 2008 9.3
Jobbörse 7.5; 10.5.1
Journalisten 4.7.3.2
Kennzeichnungspflichten 2.3; 3.1; 3.4.5; 8.5
Kernbereich der privaten Lebensgestaltung 4.1 ff.; 4.3.1
Kinder 2.9; 13.9
Kleiderkasse (der Bundeswehr) 16.11
KombiFiD 5.4
Kontenabrufverfahren 9.4
Kraftfahrt-Bundesamt (KBA) 12.3
Krankenkasse 10.2 ff.; 16.13
Krankenversichertenkarte 6.1.2
Krankenversicherung 10.2 ff.; 13.2.1
Krankenversicherungskernbereich – KAN 13.7
Kundenbindungsprogramm 3.1
Kundendaten 8.5

Lissabon-Vertrag 13.1; 13.3.8
Listenprivileg 3.4.5
Lohnsteuerabzugsmerkmale 9.3
Luftfahrt-Bundesamt (LBA) 16.17
Luftfahrt-Bundesamt (LBA) 16.17
Luftfahrt-Bundesamt (LBA) 16.17
Luftfahrt-Bundesamt (LBA) 16.17
Luftfahrt-Bundesamt (LBA) 16.17
Luftfahrt-Bundesamt (LBA) 16.17
Luftfahrt-Bundesamt (LBA) 16.17
Luftfahrt-Bundesamt (LBA) 16.17

Mautdaten 12.1
MEDICI 3.3.1
Melderechtsummengesetz 5.2; 6.5; 9.1
Melderechtsreform 5.2; 6.5
Melderegister 5.2; 6.5; 9.1
Melderegisterauskunft 5.2
Meldewesen 5.2; 6.5
Migrationshintergrund 10.5.2
Mikrodaten 5.3 ff.
Militärischer Abschirmdienst (MAD) 4.7.2
Mitarbeiterüberwachung 11.1
Mobilfunkortung 7.7

Nachrichtenaustausch 13.7
Nachrichtendienste 4.1.3; 4.2; 4.2.1; 4.2.2.2; 4.7
Nutzungsdaten 7.9

Öffentliche Petition 16.9
Öffentlichkeitsarbeit 15.8
Olivennes-Vereinbarung 7.4
Online-Durchsuchung 1.; 4.1 ff.; 4.3.1; 8

Opt-In 8.5
Outsourcing 2.5; 2.6
Patientendaten 6.1.1
Pay as You Drive 16.18
Personal beim BfDI 15.11
Personal-, Organisations- und Stellenmanagementsystem EPOS 2.0 16.14
PIN AG 3.3.2
PNR-Daten 13.5 ff.
Polizei 4.2.1; 4.2.2.2; 13.3
Polizeibehörde 4.2
Polizeiliche und justizielle Zusammenarbeit 13.3.1; 13.3.8
Polizeilicher Informations- und Analyseverbund (PIAV) 4.3.2
Postbeschlagnahme 4.5
Postunternehmen 3.3 ff.; 4.5
Pressestelle des BfDI 15.8
Primärerhebung 5.3 ff.
Privatwirtschaft 3.1
Profilbildung 3.4.4
Programm rsCASE 4.2.4
Projekt D115 2.7
Projekt GanGEs 6.4; 13.3.7
Protokollierung 4.2.2.1; 4.3.2.1
Prümer Vertrag 13.3.2; 13.3.8; 13.4
PSIS 8.1
Publikationspflichten 3.4.3
Push-Verfahren 13.5.1
Quellen-Telekommunikationsüberwachung 4.1; 4.1.1

Rasterfahndung 4.3.1
Rechtsanwälte 3.4.6
Rehabilitation 10.4; 16.13
Rentenversicherung 10.4
RFID (Radio Frequency Identification) 6.7
Risikostrukturausgleich 10.2.3
Rufnummer 3.2.4; 16.25
Russische Föderation 13.7
Safe Harbor 13.2.2
Schadsoftware 8.4
Schengen 13.3.4; 13.3.8
Schengener Informationssystem 13.3.4
Schutzmechanismen 8.4
Schwarzarbeitsbekämpfungsverordnung 16.5
Schwedische Initiative 13.3.6
Schweigepflicht 2.6
Schweigepflichtsentbindungserklärung 14.1
Score-Verfahren 3.4.4
Score-Wert 3.4.4
Sekundärhebung 5.3 ff.
Sendungsdaten 3.3.1
Sicherheitsarchitektur 4.2; 4.2.2.2
Sicherheitsbehörden 4.1; 13.3; 13.3.5; 13.3.8
Sicherheitssoftware 8.4
Sicherheitsüberprüfung 4.8.1; 4.8.2; 4.8.3
Sicherheitsüberprüfungsgesetz (SÜG) 4.8.3
SIS I+ 13.3.4; 13.3.8
SIS II 13.3.4
SIS one 4All 13.3.4
Soziale Netzwerke 7.3; 13.9
Sozialhilfeempfänger 6.1.2
Statistik 5.3 ff.
Statistisches Bundesamt 5.4.1; 5.4.2; 16.19
Steueridentifikationsnummer 9.1
Steuerungsmaßnahmen 10.2.1
Strafmündige 4.3.2.2
Strafverfolgungsbehörden 13.3.1; 13.3.6
Strafverfolgungszwecke 13.5.2
Straßenverkehrsinformationen 7.8
Street View 7.2
Suchdienstedatenschutzgesetz 16.4
Suchmaschinen 7.6

Technologischer Datenschutz 8
Telearbeit 11.4
Telefonbuch 3.2.4
Telefonbucheinträge 3.2.4
Telefonkunden 3.2.5
Telekommunikationsdienstanbieter 3.2 ff; 16.25
Telekommunikationsrichtlinien 7.12
Telekommunikationsüberwachung 4.2.1; 4.5; 5.1
Telekommunikationsunternehmen 3.2 ff.; 7.8
Telekommunikationsverkehrsdaten 3.2.2; 7.8
Telematikverfahren 16.18
Telemediengesetz 7.9
Terrorismusbekämpfungsgesetz 4.2
terrorlisten 13.6
TNT Post 3.3.2
Trennungsgebühr 4.2; 4.2.1
ubiquitous computing 1
Übermittlungssperren 9.1
Unfallversicherungsträger 10.3.1; 10.3.2
Unterrichtungspflicht 2.8
UPS-Gruppe 16.15
Urheberrechtsverletzungen 7.4
Verbindungsbüro des BfDI 15.9
verdeckte Speicherung 4.2.2.1
Vereinte Nationen 13.6
Verfügbarkeitsprinzip 13.8
Verhaltensregeln 3.4.7
Verkehrsdetektion 3.2.2; 7.8; 7.12
Verkehrsdatenabfrage 5.1
Verschlüsselung 8.2
Verschlüsselungsprogramme 8.2
Versichertestatus 6.1.2
Versicherungswirtschaft 3.4.7
Versorgungsverwaltung 10.2.1
Vertrag von Lissabon 13.1; 13.3.8
Vertrag von Prüm 13.3.2; 13.3.8; 13.4
Vertragsloser Zustellverkehr 16.12
Verwaltungsmodernisierung 2.5
Video-Infozeichen 8.1
Videoüberwachung 4.4.2; 8.1
Videoüberwachungsanlagen 8.1
Virtueller Arbeitsmarkt 7.5
Visa-Informationssystem 5.7; 13.3.5
VIS-Zugangsbeschluss 13.3.5
VIS-Zugangsgesetz 13.3.5
Volkszählung 2011 5.5
Volltextsuche 3.4.3
vorbeugender personeller Sabotageschutz 4.8.2; 4.8.3
Vorratsdaten 7.4

Web 2.0 7.3
Wehrpflichtige 14.1
Werbewiderspruch 2.8
Werbwirtschaft 3.4.5
Werbezwecke 3.4.5
Wirtschaft 3.1
Wirtschaftsprüferkammer 3.4.1

Wissenschaftsserver 16.19
Working Party on Police and Justice (WPPJ) 13.3.3; 13.3.8

ZAG (Zentren für Arbeit und Grundsicherung) 10.5.3
Zensus 2011 5.5
Zensusvorbereitungsgesetz 5.5.1
Zentrales Fahrerlaubnisregister 12.3
ZIS 13.3.8
Zollfahndungsdienstgesetz 13.7; 16.23
Zollinformationssystem 13.3.8
Zusatzversicherung 10.2.4
Zuverlässigkeitsüberprüfung 4.8.3; 4.8.3.1; 4.8.3.2
### Abkürzungsverzeichnis/Begriffe

<table>
<thead>
<tr>
<th>Abkürzung</th>
<th>Begriff</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>Auswärtiges Amt</td>
</tr>
<tr>
<td>a. a. O</td>
<td>am angegebenen Orte</td>
</tr>
<tr>
<td>ABl.</td>
<td>Amtsblatt der Europäischen Gemeinschaften</td>
</tr>
<tr>
<td>ABMG</td>
<td>Autobahnmautgesetz</td>
</tr>
<tr>
<td>Abs.</td>
<td>Absatz</td>
</tr>
<tr>
<td>AFIS</td>
<td>Automatisches Fingerabdruck-Identifizierungssystem</td>
</tr>
<tr>
<td>AG</td>
<td>Aktiengesellschaft, aber auch: Arbeitsgruppe</td>
</tr>
<tr>
<td>AG</td>
<td>Amtsgericht</td>
</tr>
<tr>
<td>AGB</td>
<td>Allgemeine Geschäftsbedingungen</td>
</tr>
<tr>
<td>ALG II</td>
<td>Arbeitslosengeld II</td>
</tr>
<tr>
<td>Alt.</td>
<td>Alternative</td>
</tr>
<tr>
<td>AO</td>
<td>Abgabenordnung</td>
</tr>
<tr>
<td>API</td>
<td>Advance passenger information</td>
</tr>
<tr>
<td>ARGE</td>
<td>Arbeitsgemeinschaften nach dem Sozialgesetzbuch II</td>
</tr>
<tr>
<td>Art.</td>
<td>Artikel</td>
</tr>
<tr>
<td>ATDG</td>
<td>Antiterrordategesetz</td>
</tr>
<tr>
<td>AufenthG</td>
<td>Aufenthaltsgesetz</td>
</tr>
<tr>
<td>AufenthV</td>
<td>Aufenthaltsverordnung</td>
</tr>
<tr>
<td>AuslG</td>
<td>Ausländergesetz</td>
</tr>
<tr>
<td>AVV</td>
<td>Allgemeine Verwaltungsvorschrift</td>
</tr>
<tr>
<td>AWG</td>
<td>Außenwirtschaftsgesetz</td>
</tr>
<tr>
<td>Az.</td>
<td>Aktenzeichen</td>
</tr>
<tr>
<td>AZR</td>
<td>Ausländerzentralregister</td>
</tr>
<tr>
<td>AZRG</td>
<td>Gesetz über das Ausländerzentralregister</td>
</tr>
<tr>
<td>BA</td>
<td>Bundesagentur für Arbeit</td>
</tr>
<tr>
<td>BAC</td>
<td>Basic Access Control</td>
</tr>
<tr>
<td>BaFin</td>
<td>Bundesanstalt für Finanzdienstleistungen</td>
</tr>
<tr>
<td>BAuG</td>
<td>Bundesausbildungsförderungsgesetz</td>
</tr>
<tr>
<td>BAG</td>
<td>Bundesamt für Güterverkehr</td>
</tr>
<tr>
<td>BAKöV</td>
<td>Bundesakademie für öffentliche Verwaltung</td>
</tr>
<tr>
<td>BAMF</td>
<td>Bundesamt für Migration und Flüchtlinge</td>
</tr>
<tr>
<td>BAN</td>
<td>Bundespolizeiaktenachweis</td>
</tr>
<tr>
<td>BArchG</td>
<td>Bundesarchivgesetz</td>
</tr>
<tr>
<td>BAZ</td>
<td>Bundesamt für den Zivildienst</td>
</tr>
<tr>
<td>BBG</td>
<td>Bundesbeamten gesetz</td>
</tr>
<tr>
<td>BCR</td>
<td>Binding Corporate Rules; verbindliche unternehmensinterne Datenschutzregelungen</td>
</tr>
<tr>
<td>bdDSB</td>
<td>behördlicher Datenschutzbeauftragter</td>
</tr>
<tr>
<td>BDSG</td>
<td>Bundesdatenschutzgesetz</td>
</tr>
<tr>
<td>BiDI</td>
<td>Bundesbeauftragter für den Datenschutz und die Informationsfreiheit</td>
</tr>
</tbody>
</table>
BfD/BA  Beauftragter für den Datenschutz der Bundesanstalt für Arbeit
BJ  Bundesamt für Justiz
BfV  Bundesamt für Verfassungsschutz
BGBl.  Bundesgesetzblatt
BKA  Bundeskriminalamt
BKAG  Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
Bluetooth  Standard für die drahtlose Übermittlung von Sprache und Daten im Nahbereich
BMAS  Bundesministerium für Arbeit und Soziales
BMF  Bundesministerium der Finanzen
BMFSFJ  Bundesministerium für Familie, Senioren, Frauen und Jugend
BMG  Bundesministerium für Gesundheit
BMI  Bundesministerium des Innern
BMJ  Bundesministerium der Justiz
BMWBW  Bundesministerium für Verkehr, Bau- und Wohnungswesen
BMVg  Bundesministerium der Verteidigung
BMWi  Bundesministerium für Wirtschaft und Technologie
BND  Bundesnachrichtendienst
BNDG  Gesetz über den Bundesnachrichtendienst
BPol  Bundespolizei
BPolG  Bundespolizeigesetz
BR  Bundesrat
BSI  Bundesamt für Sicherheit in der Informationstechnik
BSIe  Bundesbundesministerium für Familie, Senioren, Frauen und Jugend
BStU  Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT  Bundestag
BVA  Bundesverwaltungsamt, aber auch: Bundesversicherungsamt
BVerfG  Bundesverfassungsgericht
BVerfGE  Entscheidungen des Bundesverfassungsgerichts
BVerfSchG  Bundesverfassungsschutzgesetz
BVerwG  Bundesverwaltungsgericht
BVV  Bundesvermögensverwaltung
BZR  Bundeszentralregister
BZRG  Bundeszentralregistergesetz
BZSt  Bundeszentralamt für Steuern
bzw.  beziehungsweise
ca.  circa

CC  Common Criteria
CD/CD-ROM  Compact Disc - Read Only Memory

DB  Deutsche Bahn
d. h.  das heißt

DDR Deutsche Demokratische Republik
DMP Disease-Management-Programme
DNA Desoxyribonuclein acid (acid=Säure)
Dok. Dokument
DRM Digital Rights Management (Digitales Rechte Management)
Drs. Drucksache
Düsseldorfer Kreis Koordinierungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich
DV/dv Datenverarbeitung

EAC Extended Access Controll
e. V. eingetragener Verein
E-Commerce Elektronik Commerce/Elektronischer Handel
ED Erkennungsdienst
EDPS Europäischer Datenschutzbeauftragter
EDV Elektronische Datenverarbeitung
EG Europäische Gemeinschaft(en)
EG-ZIS Europäisches Zollinformationssystem
EHUG Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister
EJG Eurojust-Gesetz
ELEN Elektronischer Einkommensnachweis (JobCardverfahren)
ELSTER Elektronische Steuererklärung
E-Mail Electronic Mail
EP Europäisches Parlament
E-PA Elektronischer Personalausweis
EPOS Elektronisches Personal-, Organisations- und Stellenmanagement-System
EstG Einkommensteuergesetz
ETB Elektronisches Tagebuch
etc. etcetera
eTIN Lohnsteuerliches Ordnungsmerkmal
EU Europäische Union
EuGH Europäischer Gerichtshof
Eurodac Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern
EUROPOL Europäisches Polizeiamt
EVN Einzelverbindungsnachweis
EWG Europäische Wirtschaftsgemeinschaft
EWR Europäischer Wirtschaftsraum

f. folgend
FDZ Forschungsdatenzentrum
ff. folgende
FH Bund Fachhochschule des Bundes für öffentliche Verwaltung
FIDE | automatisiertes Aktennachweissystem im Zollbereich
---
FIFA | Fédération Internationale de Football Association
FIU | Financial Intelligence Unit
FKS | Finanzkontrolle Schwarzarbeit
FVG | Finanzverwaltungsgesetz

G.10 | Artikel 10 Gesetz
GBA | Generalbundesanwalt beim Bundesgerichtshof
gem. | gemäß
GFG | Gemeinsame Finanzermittlungsgruppe
GG | Grundgesetz
ggf. | gegebenenfalls
GGO | Gemeinsame Geschäftsordnung der Bundesministerien
GK | Gemeinsame Kontrollinstanz von Europol
GKI | Gemeinsame Kontrollinstanz von Schengen
GKV | Gesetzliche Krankenversicherung
GKV-WSG | Gesetz zur Stärkung des Wettbewerbs in der Gesetzlichen Krankenversicherung
GmbH | Gesellschaft mit beschränkter Haftung
GMBI | Gemeinsames Ministerialblatt
GMG | Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
GTAZ | Gemeinsames Terrorismusabwehrzentrum
GwG | Geldwäschegesetz

HKP | häusliche Krankenpflege
HPC | Health Professional Card
html | Hypertext Markup Language
HVBG | Hauptverband der gewerblichen Berufsgenossenschaften

IATA | International Air Transport Association
i. d. F. | in der Fassung
i. S. d. | im Sinne des (der)
i. S. v. | im Sinne von
i. V. m. | in Verbindung mit
ICAO | International Civil Aviation Organization
ICHEIC | International Commission on Holocaust Era Insurance Claims
IFG | Informationsfreiheitsgesetz
IFOS-Bund | Interaktives Fortbildungssystem für die Bundesverwaltung
IHK | Industrie- und Handelskammer
IKPO | Internationale Kriminalpolizeiliche Organisation
ILO | International Labour Organization
IMK | Ständige Konferenz der Innenminister und -senatoren der Länder
IMSI International Mobile Subscriber Identity
InGe Integrationsdatei
INPOL Informationssystem der Polizei
InsO Insolvenzordnung
INZOLL Informationssystem der Zollverwaltung
IP Internet Protocol
IPR Internationales Privatrecht
IPSec Internet Protocol Security
ISDN Integrated Services Digital Network
ISO International Organization for Standardization
IT Informationstechnik
IVBB Informationsverbund Berlin-Bonn

JI-Rat Rat der Innen- und Justizminister der Europäischen Union

KBA Kraftfahrt-Bundesamt
KFU Krebsfrüherkennungsrichtlinien
Ka Kraftfahrzeug
KOM Europäische Kommission
KWG Kreditwesengesetz

LAN Local Area Network
LfD Landesbeauftragter für den Datenschutz
lit. litera (=Buchstabe)
LKA/LKÄ Landeskriminalamt/Landeskriminalämter
LuftSiG Gesetz zur Neuregelung von Luftsicherheitsaufgaben (Luftsicherheitsgesetz)

m. E. meines Erachtens
MAD Militärischer Abschirmdienst
MADG Gesetz über den MAD
MDK Medizinischer Dienst der Krankenversicherung
MRRG Melderechtsrahmengesetz
MZG Mikrozensusgesetz

NADIS Nachrichtendienstliches Informationssystem
Nr. Nummer

o. a. oben aufgeführt
o. g. oben genannt
OECD Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD Oberfinanzdirektion
OK Organisierte Kriminalität, aber auch: Organisationskomitee
<table>
<thead>
<tr>
<th>Abkürzung</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OLAF</td>
<td>Europäisches Amt für Betrugsbekämpfung</td>
</tr>
<tr>
<td>PassG</td>
<td>Passgesetz</td>
</tr>
<tr>
<td>PAVOS</td>
<td>Polizeiliches Auskunfts- und Vorgangsbearbeitungssystem (beim BGS)</td>
</tr>
<tr>
<td>PC</td>
<td>Personalcomputer</td>
</tr>
<tr>
<td>PersauswG</td>
<td>Personalausweisgesetz</td>
</tr>
<tr>
<td>PKGr</td>
<td>Parlamentarisches Kontrollgremium</td>
</tr>
<tr>
<td>PNR</td>
<td>Passenger Name Record</td>
</tr>
<tr>
<td>Protection Profile</td>
<td>Schutzprofil</td>
</tr>
<tr>
<td>Ratsdok.</td>
<td>Ratskakument (EU)</td>
</tr>
<tr>
<td>Rdn.</td>
<td>Randnummer</td>
</tr>
<tr>
<td>Reha</td>
<td>Rehabilitation</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification – Transpondertechnik für die berührungslose Erkennung von Objekten</td>
</tr>
<tr>
<td>RFID-Chip</td>
<td>Radio Frequency Identification-Chip (Funkchip)</td>
</tr>
<tr>
<td>RSAV</td>
<td>Risikostrukturausgleichsverordnung</td>
</tr>
<tr>
<td>RVOrgG</td>
<td>Organisationsreform in der gesetzlichen Rentenversicherung</td>
</tr>
<tr>
<td>S.</td>
<td>Seite</td>
</tr>
<tr>
<td>s.</td>
<td>siehe</td>
</tr>
<tr>
<td>s. o.</td>
<td>siehe oben</td>
</tr>
<tr>
<td>s. u.</td>
<td>siehe unten</td>
</tr>
<tr>
<td>SCHUFA</td>
<td>Schutzgemeinschaft für allgemeine Kreditsicherung</td>
</tr>
<tr>
<td>SchwarzArbG</td>
<td>Schwarzarbeitsbekämpfungsgesetz</td>
</tr>
<tr>
<td>SDÜ</td>
<td>Schengener Durchführungsübereinkommen</td>
</tr>
<tr>
<td>SG</td>
<td>Soldatengesetz</td>
</tr>
<tr>
<td>SGB</td>
<td>Sozialgesetzbuch</td>
</tr>
<tr>
<td>SGB I</td>
<td>Sozialgesetzbuch Erstes Buch (Allgemeiner Teil)</td>
</tr>
<tr>
<td>SGB II</td>
<td>Sozialgesetzbuch Zweites Buch (Grundsicherung für Arbeitssuchende)</td>
</tr>
<tr>
<td>SGB III</td>
<td>Sozialgesetzbuch Drittes Buch (Arbeitsförderung)</td>
</tr>
<tr>
<td>SGB IV</td>
<td>Sozialgesetzbuch Viertes Buch (Gemeinsame Vorschriften für die Sozialversicherung)</td>
</tr>
<tr>
<td>SGB V</td>
<td>Sozialgesetzbuch Fünftes Buch (Gesetzliche Krankenversicherung)</td>
</tr>
<tr>
<td>SGB VI</td>
<td>Sozialgesetzbuch Sechtes Buch (Gesetzliche Rentenversicherung)</td>
</tr>
<tr>
<td>SGB VII</td>
<td>Sozialgesetzbuch Siebentes Buch (Gesetzliche Unfallversicherung)</td>
</tr>
<tr>
<td>SGB VIII</td>
<td>Sozialgesetzbuch Achtes Buch (Kinder- und Jugendhilfe)</td>
</tr>
<tr>
<td>SGB IX</td>
<td>Sozialgesetzbuch Neuntes Buch (Rehabilitation und Teilhabe behinderter Menschen)</td>
</tr>
<tr>
<td>SGB X</td>
<td>Sozialgesetzbuch Zehntes Buch (Sozialverwaltungsverfahren und Sozialdatenschutz)</td>
</tr>
<tr>
<td>SGB XI</td>
<td>Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung)</td>
</tr>
<tr>
<td>SGB XII</td>
<td>Sozialgesetzbuch Zwölftes Buch (Sozialhilfe)</td>
</tr>
<tr>
<td>SigG</td>
<td>Signaturgesetz</td>
</tr>
<tr>
<td>SIS</td>
<td>Schengener Informationssystem</td>
</tr>
<tr>
<td>Abk.</td>
<td>Beschreibung</td>
</tr>
<tr>
<td>------</td>
<td>--------------</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>sog.</td>
<td>so genannt</td>
</tr>
<tr>
<td>Stasi</td>
<td>Staatssicherheitsdienst der ehemaligen DDR</td>
</tr>
<tr>
<td>StDAV</td>
<td>Steuerdaten-Abruf-Verordnung</td>
</tr>
<tr>
<td>StDÜV</td>
<td>Steuerdatenübermittlungsverordnung</td>
</tr>
<tr>
<td>Steuer-ID</td>
<td>Identifikationsnummer für steuerliche Zwecke (steuerliches Identifikationsmerkmal/-nummer)</td>
</tr>
<tr>
<td>StGB</td>
<td>Strafgesetzbuch</td>
</tr>
<tr>
<td>StPO</td>
<td>Strafprozessordnung</td>
</tr>
<tr>
<td>StUG</td>
<td>Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)</td>
</tr>
<tr>
<td>StVBG</td>
<td>Steuerverkürzungsbekämpfungsgesetz</td>
</tr>
<tr>
<td>StVergAbG</td>
<td>Steuervergünstigungsabbaugesetz</td>
</tr>
<tr>
<td>StVollzG</td>
<td>Strafvollzugsgesetz</td>
</tr>
<tr>
<td>SDDSG</td>
<td>Suchdienstedatenschutzgesetz</td>
</tr>
<tr>
<td>SÜFV</td>
<td>Sicherheitsüberprüfungsfeststellungsverordnung</td>
</tr>
<tr>
<td>SÜG</td>
<td>Sicherheitsüberprüfungsgesetz</td>
</tr>
<tr>
<td>TB</td>
<td>Tätigkeitsbericht</td>
</tr>
<tr>
<td>TBG</td>
<td>Terrorismusbekämpfungsgesetz</td>
</tr>
<tr>
<td>TC</td>
<td>Trusted Computing</td>
</tr>
<tr>
<td>TK</td>
<td>Telekommunikation</td>
</tr>
<tr>
<td>TKG</td>
<td>Telekommunikationsgesetz</td>
</tr>
<tr>
<td>TOP</td>
<td>Tagesordnungspunkt</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>u. a.</td>
<td>unter anderem</td>
</tr>
<tr>
<td>u. ä.</td>
<td>und ähnliches</td>
</tr>
<tr>
<td>u. U.</td>
<td>unter Umständen</td>
</tr>
<tr>
<td>UIG</td>
<td>Umweltinformationsgesetz</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>UrhG</td>
<td>Urheberrechtsgesetz</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus – eine Schnittstelle am PC</td>
</tr>
<tr>
<td>UStG</td>
<td>Umsatzsteuergesetz</td>
</tr>
<tr>
<td>usw.</td>
<td>und so weiter</td>
</tr>
<tr>
<td>VAM</td>
<td>Virtueller Arbeitsmarkt</td>
</tr>
<tr>
<td>VBM</td>
<td>vorläufiges Bearbeitungsmerkmal</td>
</tr>
<tr>
<td>VdAK</td>
<td>Verband der Angestellten-Krankenkassen</td>
</tr>
<tr>
<td>VDR</td>
<td>Verband Deutscher Rentenversicherungsträger</td>
</tr>
<tr>
<td>VG</td>
<td>Verwaltungsgericht</td>
</tr>
<tr>
<td>vgl.</td>
<td>vergleichsweise</td>
</tr>
</tbody>
</table>
VS  Verschlußsache
VIS  Visa-Informationssystem
vpS  Vorbeugender personeller Sabotageschutz

WiMax  Wordwide Interoperability for Microwave Access
       Standard gemäß IEEE 802.16a für lokale Funknetze
WM   Weltmeisterschaft
WP   Working Paperd/Arbeitspapier
www  World wide web

XML  Extensible Markup Language

z. B. zum Beispiel
z. T. zum Teil
ZAG  Zentren für Arbeit und Grundsicherung
ZDG  Zivildienstgesetz
ZIS  Zollinformationssystem
ZStV Zentrales Staatsanwaltschaftliches Verfahrensregister
<table>
<thead>
<tr>
<th>Tätigkeitsbericht</th>
<th>Berichtszeitraum</th>
<th>Bundestagsdrucksachennummer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>1978</td>
<td>8/2460</td>
</tr>
<tr>
<td>2.</td>
<td>1979</td>
<td>8/3570</td>
</tr>
<tr>
<td>3.</td>
<td>1980</td>
<td>9/93</td>
</tr>
<tr>
<td>4.</td>
<td>1981</td>
<td>9/1243</td>
</tr>
<tr>
<td>5.</td>
<td>1982</td>
<td>9/2386</td>
</tr>
<tr>
<td>6.</td>
<td>1983</td>
<td>10/877</td>
</tr>
<tr>
<td>7.</td>
<td>1984</td>
<td>10/2777</td>
</tr>
<tr>
<td>8.</td>
<td>1985</td>
<td>10/4690</td>
</tr>
<tr>
<td>9.</td>
<td>1986</td>
<td>10/6816</td>
</tr>
<tr>
<td>10.</td>
<td>1987</td>
<td>11/1693</td>
</tr>
<tr>
<td>11.</td>
<td>1988</td>
<td>11/3932</td>
</tr>
<tr>
<td>12.</td>
<td>1989</td>
<td>11/6458</td>
</tr>
<tr>
<td>13.</td>
<td>1990</td>
<td>12/553</td>
</tr>
<tr>
<td>15.</td>
<td>1993 – 1994</td>
<td>13/1150</td>
</tr>
<tr>
<td>17.</td>
<td>1997 – 1998</td>
<td>14/850</td>
</tr>
<tr>
<td>18.</td>
<td>1999 – 2000</td>
<td>14/5555</td>
</tr>
<tr>
<td>19.</td>
<td>2001 – 2002</td>
<td>15/888</td>
</tr>
<tr>
<td>20.</td>
<td>2003 – 2004</td>
<td>15/5252</td>
</tr>
</tbody>
</table>