

9. Inneres

9.1 Neues Gesetz über den Verfassungsschutz im Lande Bremen

Nachdem die in den Jahren 2000, 2002 und 2004 vorgesehenen Änderungen des Bremischen Verfassungsschutzgesetzes scheinbar politisch nicht durchsetzbar waren – ich habe jeweils im 25. Jahresbericht und 27. Jahresbericht über meine datenschutzrechtlichen Bedenken berichtet – hat nunmehr das Innenressort einen neuen Anlauf genommen. Grundlage ist die im Koalitionsvertrag getroffene Vereinbarung, die Zusammenarbeit mit dem niedersächsischen Landesamt für Verfassungsschutz zu intensivieren. Obwohl die damit verbundenen Pläne einer Zusammenlegung der Verfassungsschutzämter von Bremen und Niedersachsen nach bisherigem Kenntnisstand nicht mehr weiter verfolgt werden, soll scheinbar an einer Angleichung der Verfassungsschutzgesetze der beiden Länder festgehalten werden.

Für mich ist eine Angleichung kein eigener Wert: Unterschiedliche Länder – unterschiedliche politische Auffassungen von den Aufgaben und Schwerpunkten einer Verfassungsschutzbehörde. Bremen war das erste Land unter den Bundesländern mit datenschutzrechtlichen Regelungen für den Verfassungsschutz. Alle anderen Länder sind nach und nach gefolgt. Eine solche Vorbildrolle sollte Bremen weiter behalten. Auch die Zusammenarbeit der Verfassungsschutzämter von Bremen und Niedersachsen würde durch eine einheitliche Regelung nicht verbessert, denn die Zusammenarbeit unter den Verfassungsschutzämtern des Bundes und der Länder ist einheitlich durch Bundesgesetz verpflichtend geregelt. Daraus ergibt sich somit kein Änderungsbedarf.

Im Juli 2005 übersandte mir der Senator für Inneres und Sport einen neuen Entwurf eines Gesetzes über den Verfassungsschutz im Lande Bremen mit Änderungen. Die von mir im vergangenen Berichtsjahr abgegebene Stellungnahme (vgl. 27. JB, Ziff. 6.10) hatte zu mehreren Veränderungen des Entwurfs geführt. Meine verbliebenen, zum Teil gravierenden datenschutzrechtlichen Bedenken führten lediglich zu geringen Änderungen des Entwurfs, bevor im November 2005 der Senat mit dem Gesetzentwurf befasst wurde.

Zum Schutz des Kernbereichs privater Lebensgestaltung bei der Wohnraumüberwachung: Der Gesetzentwurf setzt die Vorgaben des Bundesverfassungsgerichts aus seiner Entscheidung vom 3. März 2004 (1 BvR 2378/98 und 1 BvR 19084/99) nicht vollständig um. Die Wohnraumüberwachung wird bei der Wohnung des Verdächtigen nicht auf ihn beschränkt, so dass andere Personen, die sich dort allein aufhalten, entgegen der Ansicht des Bundesverfassungsgerichts überwacht werden können. Auch können Wohnungen Dritter bereits überwacht werden, wenn die verdächtige Person sich darin aufhält, während das Bundesverfassungsgericht zusätzlich tatsächliche Anhaltspunkte verlangt hat, dass dadurch verfahrensrelevante und verwertbare Gespräche erlangt werden.

Ferner wird die Übermittlung der bei der Wohnraumüberwachung anfallenden Daten an die Strafverfolgungsbehörden in Fällen erlaubt, in denen diese die Daten nicht selbst hätten erheben können. Dies stellt nach der Rechtsprechung des Bundesverfassungsgerichts eine unzulässige Zweckänderung dar.

Schließlich soll die Wohnraumüberwachung nach dem Gesetzentwurf solange und soweit stattfinden, wie neben die Vermutung, dass dort höchstpersönliche Gespräche geführt werden, die Vermutung gesetzt werden kann, dass auch über nicht schutzwürdige strafrechtlich relevante Sachverhalte gesprochen wird. Da ein „großer Lauschangriff“ nur in Betracht gezogen werden darf, wenn vermutet wird, dadurch für die Verhinderung und Aufklärung von Straftaten wichtige Informationen zu erlangen, läuft die Formulierung darauf hinaus, dass die akustische Wohnraumüberwachung immer, d. h., unabhängig von der Art der Räume und der anwesenden Personen, angeordnet wird. Das Bundesverfassungsgericht hat dagegen ein Erhebungs- und Überwachungsverbot gefordert, wenn eine Vorabprognose nach Art der Räume und anwesenden Personen die Vermutung nahe legt, dass das Abhören zu einer Verletzung des Kernbereichs privater Lebensgestaltung führen wird.

Zur Hilfestellung bei der Verwendung von Tarnmitteln: Der Entwurf sieht für alle öffentlichen Stellen die Verpflichtung vor, dem Landesamt für Verfassungsschutz bei der Bereitstellung von Tarnmitteln Unterstützung zu leisten. Aufgrund meiner im vergangenen Berichtsjahr dargestellten Bedenken (vgl. 27. JB, Ziff. 6.10) wurde bedauerlicherweise nur in der amtlichen Begründung festgehalten, dass die Hilfeleistungspflicht lediglich die allgemeine Pflicht zur Amtshilfe ergänzt und bei einer Kollision mit den Aufgaben der verpflichteten Behörde oder Stelle ein Ausgleich gesucht wird. Es wurde ferner in der amtlichen Begründung klargestellt, dass hiermit keine Erweiterung der Kompetenzen des Landesamtes für Verfassungsschutz verbunden ist. Ob diese rechtstheoretischen Ausführungen in der Praxis tragen, erscheint fraglich.

Zu den datenschutzrechtlichen Bestimmungen im Entwurf: Der Gesetzentwurf sieht weiterhin trotz meiner wiederholten Hinweise in einigen Bereichen eigene bereichsspezifische datenschutzrechtliche Bestimmungen vor, obwohl diese bereits ausreichend im Bremischen Datenschutzgesetz (BremDSG) geregelt sind. Betroffen sind der Auskunftsanspruch sowie die Regelungen zur Berichtigung, Löschung und Sperrung personenbezogener Daten.

Zu den Minderjährigenregelungen: Der Entwurf sieht im Anschluss an meine im vergangenen Berichtsjahr geäußerten Bedenken (vgl. 27. JB, Ziff. 6.10) weiterhin eine Regelung zur Speicherung von Daten Minderjähriger vor. Diese weicht von der Regelung des Bundesverfassungsschutzgesetzes insoweit ab, als auch Informationen über verfassungsfeindliche Bestrebungen oder Tätigkeiten vor der Volljährigkeit des Betroffenen die Löschung der über ihn gespeicherten personenbezogenen Daten verhindern können. Der Gesetzentwurf schließt ebenso nur die Übermittlung personenbezogener Daten Minderjähriger vor Vollendung des 14. Lebensjahres an ausländische oder an über- oder zwischenstaatliche Einrichtungen aus, während das Bundesverfassungsschutzgesetz dies für alle Informationen vor Vollendung des 16. Lebensjahres vorsieht. Der Gesetzentwurf erlaubt also abweichend vom Bundesverfassungsschutzgesetz die Übermittlung personenbezogener Daten für das 14. und 15. Lebensjahr. Noch in der Pubertät befindliche Jugendliche können so irreversibel gebrandmarkt werden.

Zur Veröffentlichung von personenbezogenen Daten durch den Verfassungsschutz: Der Gesetzentwurf sieht für Zwecke der Öffentlichkeitsaufklärung, anders als das Bundesverfassungsschutzgesetz, die Veröffentlichung von personenbezogenen Daten durch den Verfassungsschutz vor. Dies kann dazu führen, dass Betroffene gänzlich namentlich im jährlichen

Verfassungsschutzbericht genannt werden. Aus datenschutzrechtlicher Sicht bleibt problematisch, dass vor der Veröffentlichung keine Benachrichtigung des Betroffenen vorgesehen ist, die ihn vor Überraschungen schützt oder in die Lage versetzt, auf Irrtümer und Fehler hinzuweisen (vgl. auch 27. JB, Ziff. 6.10).

Zum Schutz von Amts- und Berufsgeheimnis: Der Schutz durch ein Zeugnisverweigerungsrecht geschützter Personen ist aus datenschutzrechtlicher Sicht nicht vollständig. So ist die Informationsbeschaffung nur für bestimmte nachrichtendienstliche Mittel ausgeschlossen, im Übrigen aber im Umkehrschluss zulässig (vgl. § 8 Abs. 3).

9.2 Prüfung beim Landesamt für Verfassungsschutz

Im Berichtsjahr habe ich eine Prüfung beim Landesamt für Verfassungsschutz (LfV) vorgenommen. Schwerpunkte und Ergebnisse dieser Prüfung werden nachfolgend zusammengestellt:

Zum Abruf der Meldedaten: Seit 2002 ist das LfV durch eine entsprechende Änderung in der Meldedatenübermittlungsverordnung befugt, bestimmte Meldedaten aus dem Melderegister abzurufen. § 30 Abs. 3 des bremischen Meldegesetzes bestimmt, dass die Abrufe zu protokollieren und die Aufzeichnungen bis zum Ende des nächsten Jahres, das dem Abruf folgt, aufzubewahren sind. Eine vergleichbare Vorschrift findet sich auch in § 6 Abs. 3 des Bremischen Verfassungsschutzgesetzes. Bei der Prüfung wurde festgestellt, dass die Abrufe zwar festgehalten werden, aber die gesetzliche Frist nicht eingehalten wurde, da die Aufzeichnungen bereits nach einem Monat vernichtet wurden. Es konnten jedenfalls keine weiteren Protokollbögen vorgelegt werden. Durch dieses Vorgehen war es mir nicht möglich, zurückliegende Abrufe zu kontrollieren. Das habe ich beanstandet. Bei der Gelegenheit habe ich das LfV darauf hingewiesen, dass im Rahmen der Neukonzeption des Melderegisterverfahrens (MESO) auch die Protokollierung durch das LfV rechtskonform gestaltet und dafür gesorgt werden muss, dass die Aufzeichnungen, wie in § 30 Abs. 3 des bremischen Meldegesetzes vorgeschrieben, von der abrufenden Stelle vorgenommen werden.

Zu den Zuverlässigkeitsüberprüfungen nach dem Luftsicherheitsgesetz und nach dem Hafensicherheitsgesetz: Zu dem Prüfungszeitpunkt lagen beim LfV keine unerledigten Überprüfungsfälle vor. Auch eine Liste, die der Senator für Wirtschaft und Häfen (SfWuH) mir übersandt hatte, war bereits abgearbeitet. Deshalb konnten nur theoretische Fälle „durchgespielt“ werden (vgl. auch 26. JB, Ziff. 12). Die Überprüfungsfälle werden vom SfWuH über eine sichere E-Mail-Verbindung an das LfV übermittelt und ohne Medienbruch an das Bundesamt für Verfassungsschutz (BfV) zur Prüfung (automatisches Rasterverfahren) weitergeleitet. Das LfV erhält nach wenigen Tagen eine Liste über Negativ- bzw. Positivtreffer. Die „Negativfälle“ werden umgehend freigegeben und die „Positivfälle“ werden eingehend geprüft und bewertet. Anschließend wird der SfWuH im herkömmlichen Verfahren unterrichtet. Eine solche Handhabung ist nicht zu kritisieren.

Zu Datenschutzkonzept und Verfahrensbeschreibung: Für die Hauptanwendungen (z. B. NADIS) und die technische Struktur der DV konnten ausreichende Unterlagen und Festlegungen vorgelegt werden. Allerdings bedarf es hinsichtlich der Sicherheit (fehlende Firewall) gegenüber dem Bremischen Verwaltungsnetz (BVN) Nachbesserungen, die zurzeit vom LfV noch aufgearbeitet werden.

9.3 Änderung des Bremischen Polizeigesetzes

Im Berichtsjahr wurde mir ein neuer Entwurf zur Änderung des Bremischen Polizeigesetzes (BremPolG) zur Stellungnahme übersandt. Meine datenschutzrechtlichen und verfassungsrechtlichen Bedenken im Hinblick auf die Entscheidung des Bundesverfassungsgerichts vom 27. Juli 2005 zur Verfassungswidrigkeit des Niedersächsischen Sicherheits- und Ordnungsgesetzes führten zu verschiedenen Änderungen des Entwurfs, konnten aber in einigen wesentlichen Punkten nicht ausgeräumt werden:

Zu der überarbeiteten Regelung des Lauschangriffs: Das geltende Bremische Polizeigesetz enthielt Regelungen zur Wohnraumüberwachung, die nach der Rechtsprechung des Bundesverfassungsgerichts vom 3. März 2004 (1 BvR 2378/98 und 1 BvR 19084/99) verfassungswidrig waren. Ich hatte mich mit dem Senator für Inneres und Sport darauf verständigt, dass die verfassungswidrigen Regelungen bis zu einer Neuregelung von der Polizei Bremen nicht angewendet würden. Auch die jetzt vorgeschlagenen Regelungen entsprechen leider nicht in vollem Umfang den vom Verfassungsgericht vorgegebenen Maßgaben.

So hat die Wohnraumüberwachung von vornherein zu unterbleiben, wenn Anhaltspunkte dafür bestehen, dass die Überwachung zu einer Verletzung des Kernbereichs privater Lebensgestaltung führen wird. Ergeben sich Anhaltspunkte dafür, dass Äußerungen erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, so ist die Überwachung unverzüglich abubrechen. Beides sieht der Gesetzentwurf nicht vor. Darüber hinaus nimmt der Gesetzentwurf Gespräche über Straftaten pauschal vom Kernbereich der privaten Lebensgestaltung aus. Das Bundesverfassungsgericht hingegen hat differenziert: Nicht jedwede Verknüpfung zwischen der Äußerung und dem Verdacht einer Straftat genügt. Auch der Erste Strafsenat des Bundesgerichtshofs hat in einem Urteil vom 10. August 2005 (1 StR 140/05) noch einmal bekräftigt, dass ein Selbstgespräch im Krankenzimmer in den absolut geschützten Kernbereich privater Lebensgestaltung fällt und auch bei überwiegendem allgemeinen Interesse nicht abgehört werden darf.

Bedenklich ist, dass die Gesetzesbegründung die Übertragung der vom Bundesverfassungsgericht aufgestellten Grundsätze zur repressiven Wohnraumüberwachung auf die präventive Wohnraumüberwachung verneint, da hier Zweck der Maßnahme der Schutz einer Person vor Gefahren für Leib, Leben oder Freiheit sei. Soweit ein Verursacher insoweit in Rechte Dritter eingreife, könne er keinen unantastbaren Kernbereich privater Lebensgestaltung beanspruchen. Der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung unterscheidet jedoch nicht zwischen präventiven oder repressiven Maßnahmen der Wohnraumüberwachung. Der Schutz gilt gleichermaßen, wie das Bundesverfassungsgericht auch in seinem Urteil vom 27. Juli 2005 (1 BvR 668/04) deutlich gemacht hat.

Zur Ausweitung der Identitätsfeststellung: Der Entwurf erlaubt die Identitätsfeststellung an von der Polizei festgelegten „Gefahrenorten“, wenn eine Person diesen Ort betritt oder überquert. Bislang war erforderlich, dass die Person sich vor Ort aufhält, d. h. verweilt. Durch die Ausweitung des Anwendungsbereichs werden eine Vielzahl von Personen der Möglichkeit einer Identitätsfeststellung

unterworfen, die in ihr Recht auf informationelle Selbstbestimmung eingreift. Für den Bürger ist die polizeiliche Festlegung als „Gefahrenort“ nicht erkennbar. Es ist für ihn nicht überprüfbar, ob die Polizei die Befugnis zur Identitätsfeststellung besitzt. Zur Identitätsfeststellung ist die Polizei zudem zu weiteren Maßnahmen ermächtigt. Sie darf u. a. die Person festhalten und mitgeführte Sachen nach Gegenständen durchsuchen, die der Identitätsfeststellung dienen, sowie sich mitgeführte Ausweispapiere aushändigen lassen oder die Person für erkennungsdienstliche Maßnahmen zur Dienststelle bringen.

Zur Ausweitung von Befragung und Auskunftspflichten: Durch den Gesetzentwurf wird die Befugnis der Polizei eingeführt, zur Verhütung von Straftaten von erheblicher Bedeutung in organisierter Begehungsform auch außerhalb von „Gefahrenorten“ oder Kontrollstellen Personen anzuhalten, zu befragen, mitgeführte Ausweispapiere zu prüfen und Sachen in Augenschein zu nehmen, ohne dass auf die betroffene Person bezogene Anhaltspunkte für die Begehung der Straftat vorliegen müssen. Auch hier geraten viele harmlose Personen in das Visier der Polizei, die Eingriffe in ihr Persönlichkeitsrecht hinnehmen müssen.

Zur Ausweitung von Kontrollstellen: Die Errichtung von Kontrollstellen, die eine Identitätsfeststellung erlauben, wird in dem Gesetzentwurf erheblich erweitert. Kontrollstellen dürfen bei Straftaten von erheblicher Bedeutung errichtet werden. Hierunter fallen alle Verbrechen nach dem Strafgesetzbuch, aber auch eine Reihe von Vergehen. An den Kontrollstellen werden eine Vielzahl von Personen erfasst, die mit der Straftatbegehung in keinerlei Zusammenhang stehen. Datenschutzrechtlich ist problematisch, dass die dabei erhobenen Daten erst spätestens nach einem Monat gelöscht werden sollen und nicht in jedem Fall unverzüglich, wenn keine Anhaltspunkte für die Beteiligung an einer Straftat vorliegen. Die personenbezogenen Daten sollen nach dem Gesetzentwurf zudem auch zur Verfolgung einer nicht nur geringfügigen Ordnungswidrigkeit genutzt werden. Da eine Kontrollstelle zur Verfolgung von Ordnungswidrigkeiten nicht errichtet werden darf, bestehen Zweifel, ob die erhobenen personenbezogenen Daten nicht über den Zweck hinaus verarbeitet werden, für den sie erhoben werden durften. Das Bundesverfassungsgericht hat festgehalten, dass die Weiterverwendung von Daten nur für Zwecke verfassungsmäßig ist, die auch als Rechtfertigung für die ursprüngliche Erhebung ausgereicht hätten.

Zur Videoaufzeichnung für die Eigensicherung: Der Gesetzentwurf sieht vor, dass Polizeibeamte zu ihrer Eigensicherung bei Verkehrskontrollen offen Bildaufzeichnungen anfertigen dürfen. Ich habe erreicht, dass die Aufzeichnungen nur zur Verfolgung von Straftaten gegen die Polizeibeamten, nicht auch Ordnungswidrigkeiten, verwendet werden dürfen und ansonsten unverzüglich zu löschen sind.

Zum elektronischen Kfz-Kennzeichenabgleich: Der Gesetzentwurf erlaubt der Polizei, bei Verkehrskontrollen Kfz-Kennzeichen elektronisch zu erfassen und mit dem Fahndungsdatenbestand der Polizei abzugleichen. Aufgrund meiner Intervention darf der Abgleich nur sofort erfolgen. Die Kfz-Kennzeichen aller vorbeifahrenden Fahrzeuge dürfen nicht auf Vorrat gespeichert werden.

9.4 Fotos der Polizei in der „Galerie des Verbrechens“

Im November 2004 veröffentlichte eine Boulevardzeitung in Bremen unter der Überschrift „Die Galerie des Verbrechens“ Name und Täter- bzw. Tatverdächtigenbilder, die identisch mit Bildern waren, die im Rahmen erkennungsdienstlicher Maßnahmen durch die Polizei angefertigt worden waren. Die wiedergegebenen Zahlen über Straftaten entsprachen in weiten Teilen kriminalpolizeilichen Unterlagen, die in ExtraPol abrufbar waren. Bei der prangerartigen Veröffentlichung handelt es sich um einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen. Meine auch von Seiten des behördlichen Beauftragten für den Datenschutz der Polizei Bremen unterstützten Nachforschungen, wer für die Indiskretionen verantwortlich ist, waren leider nicht erfolgreich. Die Bilder und zugehörigen personenbezogenen Daten waren auch in ExtraPol gespeichert. Daher konnte der potentielle Kreis der dafür in Frage kommenden Personen nicht eingegrenzt werden. ExtraPol ist eine gemeinsame von der Polizei im Bund und in den Ländern geführte Informationsplattform. Diese enthielt zunächst nur polizeiliche Fachinformationen (Dienstvorschriften, Fachdokumente), nahm jedoch im Jahr 2004 in einem weiteren Schritt auch fallbezogene Fahndungsdaten auf. Aus Sicht des Datenschutzes ist kritisch zu beurteilen, dass ExtraPol keine Zugriffsprotokollierung vorsieht oder in anderer Weise Downloads oder das Ausdrucken von Daten verhindert. Die datenschutzrechtlich geforderte Verantwortung einer Stelle ist damit nicht gewährleistet. Konsequenterweise hat der Polizeipräsident daraufhin eine weitere Einspeicherung von personenbezogenen Daten durch die Polizei Bremen in ExtraPol vorerst gestoppt. Nunmehr besteht die bundesweite Planung, das ExtraPol-Verfahren insgesamt zu prüfen und den datenschutztechnischen Anforderungen anzupassen.

9.5 Errichtungsanordnungen und Verfahrensbeschreibungen

Im Berichtsjahr wurde ich mit einer Reihe von Verfahrensbeschreibungen für automatisierte Verfahren bei der Polizei Bremen konfrontiert, die bereits seit längerer Zeit erlassen worden waren oder sich umgekehrt noch in einem frühen Entwurfsstadium befanden. Darunter waren z. B. die Verfahrensbeschreibungen für die Datenbank „An- und Verkaufsgeschäfte“, die Arbeitsdatei „Vermögensabschöpfung“, die Arbeitsdatei „Fahndung“, das Lagebild „Jugendkriminalität“, die Datenbank „bekannte Täter“, die so genannte "Gefährderdatei" (Stalker) und die Datenbank "Handyraub". Die Verfahrensbeschreibungen nahmen zum Teil Bezug auf überholte Rechtsvorschriften im Bremischen Datenschutzgesetz (BremDSG), Bremischen Polizeigesetz (BremPolG) oder Strafgesetzbuch (StGB). Die technischen und organisatorischen Maßnahmen nach § 7 BremDSG waren durchweg unzureichend dargestellt. Auch fehlte teilweise eine Rechtsgrundlage für den Umfang der zu speichernden Daten. Die Zugriffsberechtigten waren oft auch nicht hinreichend genau beschrieben. Ferner standen die Löschfristen nicht immer im Einklang mit den Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (so genannten KpS-Richtlinien). Alle diese Verfahrensbeschreibungen habe ich mit dem behördlichen Datenschutzbeauftragten und z. T. unter Hinzuziehung der zuständigen Fachkräfte erörtert und um Nachbesserung gebeten. Eine erneute Vorlage ist für Anfang 2006 vorgesehen.

Auch auf Bundesebene wurde ich des Öfteren aufgefordert, zu den Errichtungs- und Feststellungsanordnungen neuer personenbezogener Sammlungen des Bundeskriminalamtes, die auch die Polizei im Land Bremen nutzen, gegenüber dem Senator für Inneres und Sport eine Stellungnahme abzugeben. Dies betraf z. B. die Errichtungsanordnungen APOK, Organisierte Kriminalität Osteuropa, Geldwäschedatei, Kinderporno, Dokumente/Menschenhandel/Schleusung, Falschgeld, Waffen, FBK Tötungs- und Sexualdelikte, KAN, Personenfahndung, Sachfahndung, Erkennungsdienst, Haftdatei und Gewalttäter Sport.

9.6 ApolWeb

Bei ApolWeb handelt es sich um eine Anwendung der Ortspolizeibehörde Bremerhaven (OPB), welche ursprünglich als Rückfallebene bei Systemausfällen konzipiert war. Mit diesem System werden einmal täglich Daten aus dem örtlichen Melderegister, dem örtlichen Fahrzeugregister und dem örtlichen Fahrerlaubnisregister in einem Datenbanksystem zusammengeführt und den Beamten zum Abruf im Intranet zur Verfügung gestellt. Der behördliche Datenschutzbeauftragte legte mir die Verfahrensbeschreibung vor. Schon bald wurde der OPB deutlich, dass die Anwendung aufgrund ihrer Bedienerfreundlichkeit erhebliche Vorzüge bietet und daher nicht nur als Rückfallsystem, sondern auch für den Normalbetrieb eingesetzt werden soll. Daraus ergeben sich allerdings einige rechtliche Probleme. So dürfen nur solche Daten eingestellt werden, deren Abruf rechtlich zulässig ist. In der Datenbank sind Datenfelder enthalten, die nach der Meldedatenübermittlungsverordnung (MeldDÜV) nicht hätten zum Abruf bereit gestellt werden dürfen. Grundsätzlich ist aufgrund der Aktualität der Daten immer auf die Originaldaten zuzugreifen und aus der Protokollierung muss klar hervorgehen, welche Personen auf welche Daten zugegriffen haben.

Der Datenschutzbeauftragte der Ortspolizeibehörde Bremerhaven teilte mir zwischenzeitlich mit, dass man an einer anderen technischen Lösung arbeite, bei der die Daten im Hoheitsbereich der Verwaltungspolizei verbleiben und meine Vorgaben zum Zugriff auf die Daten eingehalten werden. Ich werde die weitere Einführung beratend begleiten.

9.7 ISAWeb

Die Polizei Bremen hat sich entschlossen, das bestehende Verfahren ISA (InformationssystemAnzeigen) auf eine neue technische Basis, nämlich webbasiert, umzustellen (vgl. 27. JB, Ziff. 6.7).

Meine datenschutzrechtlichen Anforderungen an das System habe ich der Polizei Bremen mitgeteilt. Dazu zählen unter anderem die Nachvollziehbarkeit der Datenverarbeitung, Gewährleistung der Zweckbindung, reversionssichere Protokollierung, Sicherstellung der Eindeutigkeit von Personendaten, Gewährleistung von Auskunfts- und Einsichtsrechten sowie die Festlegung der technischen- und organisatorischen Maßnahmen zum Schutz der Daten.

Im Januar 2005 wurde mir ein Prototyp der Anwendung vorgestellt. Dabei wurde mir dargelegt, an welchen Stellen das Programm inhaltlich durch neue Datenfelder ergänzt worden ist, um aus ISA (alt) bekannte Defizite auszugleichen. Ich habe keine grundsätzlichen Einwände geäußert. Weiterhin habe ich gefordert, dass die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (so genannte KpS-Richtlinien) zu aktualisieren sind. Die zurzeit gültigen Richtlinien aus dem Jahre 1981 sind veraltet und entsprechen z. B. beim Auskunftsrecht des Betroffenen oder den Aufbewahrungsfristen teilweise nicht mehr den Rechtsvorschriften.

Ich begrüße ausdrücklich, dass bei der Neugestaltung eine Schnittstelle zu der Anwendung der Staatsanwaltschaft Bremen geplant ist, die sicherstellt, dass der „Ausgang des Verfahrens“ zeitlich und rechtlich korrekt in das ISAWeb übernommen wird. Nur so können die Löschfristen exakt berechnet werden.

Im Frühjahr des Berichtsjahres habe ich um weitere Auskünfte gebeten, insbesondere um die Vorlage der Verfahrensbeschreibung mit Angabe der getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Daten sowie eine Beschreibung vorhandener Schnittstellen, eine Darstellung des Zugangs- und Zugriffsverfahrens sowie die Ausarbeitung eines Rollenkonzepts, aus dem hervorgeht, in welcher Weise und in welchem Umfang Berechtigungen im ISAWeb vergeben werden.

Die Inbetriebnahme des Programms erfolgte im Juli, ohne dass mir bis dahin die Verfahrensbeschreibung und das Fachdatenschutzkonzept zugegangen sind. Nachdem ich diese Angaben auch bis zum Herbst nicht erhalten habe, wurde das Thema im November im Rechtsausschuss der Bremischen Bürgerschaft behandelt.

Zwischenzeitlich ist die Verfahrensbeschreibung zu ISAWeb eingegangen. Eine Stellungnahme zum rechtlichen Teil ist bereits erfolgt. Es fehlte die zur Bewertung notwendige Beschreibung der Datensatzstruktur, die von der Polizei Bremen noch nachgereicht werden muss. Eine Stellungnahme zu den technischen und organisatorischen Maßnahmen befindet sich in Arbeit. Insgesamt lässt sich bereits feststellen, dass weitere Angaben erforderlich sind, insbesondere zur Softwarearchitektur und den eingesetzten Produkten, zum Beantragungsverfahren für Berechtigungen und zum Berechtigungskonzept, zur Beschreibung der Schnittstellen sowie zur Zugriffskontrolle und Eingabekontrolle. Es wurden keine Aussagen zur Zutritts-, Weitergabe- und Verfügbarkeitskontrolle

gemacht, die zu ergänzen sind. Ich erwarte, dass eine baldige Vervollständigung der Unterlagen durch die Polizei Bremen erfolgt.

9.8 Datenschutzkonzepte bei der Ortspolizeibehörde Bremerhaven

Die Ortspolizeibehörde Bremerhaven hat mir im Berichtsjahr mehrere Beschreibungen zu DV-Verfahren vorgelegt. Insgesamt musste ich feststellen, dass insbesondere Maßnahmen mit übergreifendem Charakter sowie die DV-Infrastruktur nicht ausreichend beschrieben waren. Ich habe daher zur weiteren Vorgehensweise den Vorschlag unterbreitet, alle Maßnahmen, die bezogen auf die Behörde für alle Verfahrensbeschreibungen auf technischer Ebene bei der Verwendung gleicher Sicherheitsmechanismen identisch sind, in einem „Allgemeinen Datenschutz- und Sicherheitskonzept“ zusammenzufassen. Die Erstellung dieses übergreifenden Konzeptes hat den Vorteil, dass bei Änderungen der DV-Technik (z. B. bei der Durchführung von Datensicherungen) der Anpassungsaufwand bzgl. der Dokumentation nur an einer Stelle entsteht. Hier erwarte ich insbesondere Aussagen zur Zugangskontrolle wie auch zur Verfügbarkeits- und Weitergabekontrolle (Netzinfrastruktur, Anbindung der Außenstellen).

Der Datenschutzbeauftragte der Ortspolizeibehörde Bremerhaven hat mir bis Ende Januar 2006 eine Darstellung der allgemeinen Datenschutz- und Sicherheitsmaßnahmen der Behörde in Aussicht gestellt.

Aufbauend auf diesem Konzept sollen dann in weiteren Fachdatenschutzkonzepten die Sicherheitsmechanismen dargestellt werden, die sich konkret auf die einzelnen Anwendungen und deren Implementierung beziehen. Zu ergänzen sind im Wesentlichen weitere Angaben zur Softwarearchitektur, zur Zugriffskontrolle (technischer Mechanismus zur Anmeldung und Steuerung der Zugriffe, Berechtigungskonzept, Administrationskonzept) und zur Weitergabekontrolle.

9.9 Fußball-WM 2006: Akkreditierungsverfahren

Für die Fußball-Weltmeisterschaft 2006 werden voraussichtlich mehr als 250.000 Personen, die in den Stadien tätig werden sollen, u. a. Servicebedienstete, Sicherheitskräfte, Mitarbeiter von Hilfsorganisationen und Journalisten, aber auch ehrenamtliche Helfer, Würstchen- und Fanartikel-Verkäufer, in einem Akkreditierungsverfahren durch die Sicherheitsbehörden des Bundes und der Länder auf ihre Zuverlässigkeit überprüft.

Überwiegend übermittelt der Arbeitgeber in Form von Sammelakkreditierungen der Personen, die zum Einsatz kommen sollen, Namen, Vornamen, Straße, Postleitzahl, Ort, Bundesland, Land, Geburtsdatum, -ort, -land, Nationalität, Ausweisart, -nummer und -gültigkeit an das Organisationskomitee der Veranstalter. Das Verfahren und die Kriterien, die zu einer Ablehnung führen, sind Gegenstand einer Datenschutzinformation, die der Betroffene lesen muss, bevor er in die Überprüfung einwilligen kann. Erfolgt die Übermittlung durch den Arbeitgeber, muss dieser gegenüber dem Organisationskomitee der Veranstalter erklären, dass die Arbeitnehmer entsprechend der Datenschutzinformation belehrt wurden.

Das Organisationskomitee übermittelt die für die Überprüfung erforderlichen Daten an das Bundeskriminalamt, das die Daten nach dem Wohnortprinzip in Länderpakete an die Polizei sowie Pakete für das Bundesamt für Verfassungsschutz, die Bundespolizei und das Bundeskriminalamt aufteilt und verteilt. Das Bundesamt für Verfassungsschutz verteilt seinen Datensatz wiederum nach dem Wohnortprinzip an die Landesämter für Verfassungsschutz. Die Sicherheitsbehörden überprüfen die Daten bei der Entgegennahme auf ihre Plausibilität, etwa Schreibfehler und Zahlendreher, und weisen sie ggf. zurück. Die qualifizierten Voten der Sicherheitsbehörden (akkreditiert/nicht akkreditiert) werden nach der Überprüfung ohne Begründung wieder an das Bundeskriminalamt übermittelt, das ein Gesamtvotum erstellt und dem Organisationskomitee mitteilt. Die Ablehnung einer einzelnen Sicherheitsbehörde führt zu einem ablehnenden Gesamtvotum für die betroffene Person. Dem Organisationskomitee werden weder die Gründe noch die ablehnende Sicherheitsbehörde genannt. Das Organisationskomitee teilt das Ergebnis bei Einzelakkreditierungen den Betroffenen persönlich, bei Sammelakkreditierungen hingegen dem Arbeitgeber mit, der seinerseits den betroffenen Arbeitnehmer informiert.

Die Sicherheitsüberprüfung und die vorherige Benachrichtigung des Arbeitgebers bedeuten für die Betroffenen einen erheblichen Eingriff in ihr Grundrecht auf informationelle Selbstbestimmung. Das Negativvotum führt zu einem partiellen Berufsausübungsverbot für die Betroffenen, bei Arbeitnehmern droht der Arbeitsplatzverlust, so dass auch das Grundrecht der Berufsfreiheit und bei Journalisten die Presse- und Rundfunkfreiheit berührt sind. Das Überprüfungsverfahren erweist sich aus datenschutzrechtlicher Sicht in mehrerlei Hinsicht als bedenklich:

Fehlende gesetzliche Eingriffsgrundlage: Die gesetzlichen Voraussetzungen für eine Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) liegen nach Auffassung aller Beteiligten nicht vor. Die Einwilligung der Betroffenen stellt keine ausreichende Rechtsgrundlage für eine Überprüfung durch den Verfassungsschutz oder in diesem Ausmaß durch die Polizeibehörden

dar. So fehlt es z. B. für die Beteiligung des Verfassungsschutzes an einer Zuverlässigkeitsüberprüfung bereits an einer Aufgabenzuweisung im Bremischen Verfassungsschutzgesetz. Eine Einwilligung kann dies nicht ersetzen. Die allein auf der Einwilligung der Betroffenen beruhende Sicherheitsüberprüfung ist ein Präzedenzfall und umgeht die strenge Zweckbindung der von den beteiligten Verfassungsschutzbehörden mit nachrichtendienstlichen Mitteln erlangten Erkenntnisse, die für die Überprüfung herangezogen werden. Da diese Erkenntnisse den Betroffenen nicht bekannt sind, scheidet auch insoweit eine Einwilligung aus.

Fehlende Authentizität und Wirksamkeit der Einwilligung: Das Akkreditierungsverfahren gewährleistet nicht die Authentizität der Einwilligungserklärung. Die Betroffenen erklären ihre Einwilligung in die Durchführung des Akkreditierungsverfahrens selbst oder über ihren Arbeitgeber mittels eines Online-Antragsformulars gegenüber dem Organisationskomitee. Die Sicherheitsbehörden erhalten damit keinen authentischen Nachweis, der die Urheberschaft des Einwilligenden sicherstellt. Im Prinzip könnte man so Freunde und Bekannte mit überprüfen lassen. Zweifel sind auch an der Freiwilligkeit und damit Wirksamkeit der Einwilligungserklärung angebracht. Eine Vielzahl von Arbeitnehmern wird die Erklärung nur deswegen abgeben, um negative Folgen im Arbeitsverhältnis zu vermeiden, da die fehlende Einwilligung zwingend zur Ablehnung der Akkreditierung führt.

Fehlende Verhältnismäßigkeit: Für die ablehnende Empfehlung der Sicherheitsbehörden des Bundes und der Länder genügt das negative Votum eines einzelnen Landeskriminalamtes oder Landesamtes für den Verfassungsschutz. Berücksichtigt werden auch Erkenntnisse aus eingestellten Ermittlungsverfahren oder Strafverfahren ohne gerichtliche Verurteilung. Bei den Verfassungsschutzbehörden genügt sogar der Verdacht einer Bestrebung gegen die freiheitlich demokratische Grundordnung für eine zwingende Ablehnung. Im Zweifel soll aus Gründen der Sicherheit eine Ablehnung erfolgen. So wurde bei der Endrundenauslosung zur Fußball-Weltmeisterschaft 2006 im Dezember 2005 mehrfach die Akkreditierung verweigert, weil der Personalausweis oder Reisepass des Betroffenen zu einem früheren Zeitpunkt als verloren oder gestohlen gemeldet war. Dies scheint im Hinblick auf die unter Umständen gravierenden Folgen der Nicht-Akkreditierung und dem rechtsstaatlichen Verhältnismäßigkeitsgrundsatz bedenklich.

Defizite beim Rechtsschutz: Die von den Datenschutzbeauftragten des Bundes und der Länder geforderte Rückmeldung der Ergebnisse zunächst an den Betroffenen wurde abgelehnt. Das Organisationskomitee teilt bei Sammelakkreditierungen nur dem Arbeitgeber ohne Begründung mit, dass die Akkreditierung verweigert wird. Dem betroffenen Arbeitnehmer drohen damit berufliche oder wirtschaftliche Nachteile, bevor er die Möglichkeit erhält, Fehlinformationen zu korrigieren oder Stellung zu nehmen.

Der Rechtsschutz der Betroffenen ist zudem sehr umständlich organisiert. Für den Betroffenen ist nicht erkennbar, welche Stelle für die Nicht-Akkreditierung wegen Sicherheitsbedenken verantwortlich ist. Nach außen tritt das Organisationskomitee in Erscheinung, das seine Ablehnung nicht begründet. Der Betroffene muss sich an das Landeskriminalamt seines Landes wenden, das über das Bundeskriminalamt die für die Ablehnung verantwortliche Stelle anspricht, z. B. das Bundesamt für Verfassungsschutz, das sich seinerseits an das entsprechende Landesamt für Verfassungsschutz wendet. Kritisch zu betrachten ist auch, dass die Polizeibehörden (Bundes-, Landeskriminalamt) auf

diese Weise Kenntnis erlangen, dass Informationen über den Betroffenen beim Verfassungsschutz vorliegen.

9.10 Mobile Videoüberwachung durch die Polizei

Es bestehen Planungen bei der Polizei, Videoüberwachung künftig auch mobil einzusetzen. Soweit es sich um die mobile Videoüberwachung zum Zwecke der Eigensicherung der eingesetzten Polizeibeamten handelt, verweise ich auf Ziff. 9.3 dieses Berichts. Daneben bestehen aber auch Überlegungen, vorhandene Videoüberwachungsgeräte, die gemäß § 29 Abs. 3 des BremPolG eingesetzt werden, wahlweise an verschiedenen, festgelegten Orten einzusetzen, ohne dass die begleitenden Maßnahmen, z. B. Hinweisschilder, jeweils konkret auf den Einsatz der Anlage hinweisen. Diese Pläne stehen nicht im Einklang mit § 29 Abs. 3 BremPolG; hierauf habe ich die Polizei Bremen hingewiesen.

9.11 Stalkerdatei

Im August des Berichtsjahres hat die Polizei Bremen in das Polizeiinformationssystem ISA (InformationssystemSachenAnzeigen) die Gefährderdatei „Stalker und Beziehungstäter“ eingeführt. Täter von Stalking oder häuslicher Gewalt werden im Polizeiinformationssystem mit dem personenbezogenen Hinweis „Gefährder“ aufgeführt, so dass Polizeibeamte bei ihren Einsätzen das Gefährdungspotential dieser Personen frühzeitig erkennen und entsprechend reagieren können. Das hierfür erforderliche Datenschutzkonzept wurde mit mir abgestimmt.

9.12 Datenverarbeitung bei der Feuerwehr in Bremen

Der behördliche Datenschutzbeauftragte der Feuerwehr Bremen hat mir aufgrund der Eingabe eines Mitarbeiters eine Dokumentation zur Regelung des Zugriffs auf die Dateien bei der Feuerwehr Bremen (vgl. 27. JB, Ziff. 6.14) vorgelegt. Zu diesem Konzept habe ich Stellung genommen.

Die Dokumentation ist um eine Beschreibung des Beantragungsverfahrens sowie um die Darstellung der Zugriffs- und Verzeichnisstrukturen zu vervollständigen, zur Zugangskontrolle habe ich Empfehlungen abgegeben. Weitere wesentliche Themen sind Probleme bei dezentraler Datenspeicherung (mangelnde Zugriffs- und Verfügbarkeitskontrolle), Fragen zur Vergabe von Gruppenberechtigungen sowie zu benennende Maßnahmen zur Weitergabe-, Verfügbarkeits-, Eingabe- und Auftragskontrolle. Ein Konzept zur Erhöhung der Transparenz der Administratorentätigkeit, welches beispielweise die Festlegung von Verantwortlichkeiten sowie Rechte und Pflichten, Möglichkeiten der Protokollierung und Revision darlegen soll, steht ebenfalls aus.

Zur Auftragskontrolle habe ich dargelegt, dass die Fremdwartung ein Sicherheitskonzept erfordert, durch das geeignete technische und organisatorische Maßnahmen getroffen werden, um personenbezogene Daten vor unberechtigtem Zugriff zu schützen.

Weiterhin habe ich der Bitte des Datenschutzbeauftragten der Feuerwehr Bremen entsprochen und zu Fragen der Netzwerkadministration, der Vergabe von Berechtigungen im Netz (Rollenkonzept, Zugriffskontrolle) und zu einzelnen Positionen des Netzwerksicherheitskonzeptes Stellung genommen. Der behördliche Datenschutzbeauftragte teilte mir mit, dass er voraussichtlich ab Mitte Februar 2006 Ergebnisse zu einzelnen Fragestellungen vorlegen könne.

9.13 Einsatz von Unfalldatenspeichern bei der Feuerwehr Bremen

Die Feuerwehr in Bremen informierte mich über den Einsatz von Unfalldatenspeichern, mit denen Rettungsfahrzeuge, Intensivkrankentransportwagen, Großraumkrankentransportwagen sowie Notarzteinsatzfahrzeuge ausgestattet werden. Ein Unfalldatenspeicher (UDS) ist ein Gerät, welches bei eingeschalteter Zündung permanent und uhrzeitgenau Fahrzeugbewegungen, Stellung bzw. Bedienung angeschlossener Bedienelemente erfasst und interne Vorgänge überwacht. So werden beispielsweise Daten zur Fahrzeughaltung, Quer- und Längsbeschleunigung, Geschwindigkeit, Fahrtrichtungsanzeiger, Signallicht, Blaulicht, Standlicht, Abblendlicht etc. aufgezeichnet.

Das Datenspeicherprogramm ist sehr komplex. Sobald bestimmte Merkmale erreicht sind, werden die Daten zu einem Ereignis zusammengefasst und in einem von neun Ereignisspeichern gespeichert. So sollen bei einem Unfall die letzten 28 Sekunden vor sowie 15 Sekunden nach dem Ereignis automatisch gespeichert werden. Darüber hinaus besteht die Möglichkeit, dass der Fahrzeuglenker durch Betätigung der UDS-Taste (manuelles Ereignis) die Daten der letzten 43 Sekunden und ca. 100 folgenden Meter speichert (z. B. bei dem Überfahren einer auf Rot stehenden Lichtsignalanlage). Weiterhin werden Daten in einem von drei Stillstandsspeichern gesichert, wenn das Fahrzeug länger als drei Sekunden steht, sowie interne Ereignisse (z. B. Zündung an/aus, UDS-Taste gedrückt, UDS-Speicher ausgelesen) aufgezeichnet.

Mit den UDS-Daten soll der Unfallverlauf rekonstruiert und ggf. das korrekte Verhalten der Fahrzeugführer nachgewiesen werden.

Die Daten sollen mittels eines ausschließlich hierfür vorgehaltenen Notebooks aus dem UDS heruntergeladen werden. Dieser Vorgang geschieht mit einer hierfür vorgesehenen und durch einen Hardlock gesicherten Software. Zusätzlicher Schutz des Notebooks vor missbräuchlicher Nutzung wird durch weitere technische und organisatorische Maßnahmen geschaffen. Die heruntergeladenen Daten werden auf einem kennwortgeschützten USB-Stick gespeichert und an einen vom Hersteller autorisierten und von der Feuerwehr schriftlich beauftragten Sachverständigen weitergegeben, dem die Auswertung der Daten obliegt. Die Feuerwehr Bremen besitzt keine weiterführende Software, die eine Auswertung der Daten ermöglicht.

Der Datenschutzbeauftragte der Feuerwehr Bremen legte mir die nach dem Bremischen Datenschutzgesetz (BremDSG) erforderliche Verfahrensbeschreibung sowie die Dienstanweisung und Bekanntmachung vor. Hierzu habe ich im Berichtsjahr Stellung genommen und Vorschläge und Anforderungen zur Gestaltung der Dienstvereinbarung sowie insbesondere zur Speicherung und zu den technischen und organisatorischen Maßnahmen gemacht.

Ich habe darauf hingewiesen, dass der betroffene Fahrzeugführer in jedem Fall über das Auslesen des UDS zu benachrichtigen ist. Klärungsbedarf gibt es derzeit noch zum Umfang der aufgezeichneten Betriebsdaten des Fahrzeugs wie auch zur tatsächlichen Speicherdauer und zur Löschung hoher Bewertungen. Die Messdaten werden mit einer bestimmten Bewertung durch den UDS gespeichert. Die Löschung der Daten soll durch Überschreiben der Ereignisspeicher mit einer

höheren Bewertung erfolgen. Eine abschließende Stellungnahme der Feuerwehr Bremen liegt noch nicht vor.

9.14 Internetnutzung bei der Feuerwehr Bremen

Ich habe die Feuerwehr in Bremen zur Nutzung von E-Mail und Internet am Arbeitsplatz beraten. Die mir hierzu vorgelegten Dienstvereinbarungen und Dokumente bezogen sich auf veraltete Regelwerke, was formale und inhaltliche Anpassungen erfordert hätte. Ich begrüße daher die Entscheidung der Feuerwehr Bremen, stattdessen die Richtlinie für die Nutzung der Elektronischen Post vom 7. März 2002 sowie die Richtlinie für die Bereitstellung und Nutzung von Internet-/Intranet-Zugängen vom 10. Februar 2004 einzuführen, nach dessen Vorgaben die Protokollierung ausgerichtet wird.

Hinsichtlich der Aufstellung zusätzlicher PC zur ausschließlichen privaten Nutzung des Internets habe ich auf die Einhaltung der Vorgaben zum Datenschutz und zur Protokollierung (z. B. Untersagung dezentraler Protokollierung bei privaten Zugriffen) gedrungen. So ist zu gewährleisten, dass der für die private Nutzung bereitgestellte Proxy-Server genutzt wird, ebenso müssen geeignete technische und organisatorische Maßnahmen (u. a. Firewall, Virenschutz, DMZ, logische Trennung, Deaktivierung externer Medien) getroffen werden, um das Netzwerk der Feuerwehr gegen die Internet-PC abzuschotten und vor Angriffen aus dem Internet zu schützen.

Der Datenschutzbeauftragte der Feuerwehr Bremen teilte mir mit, dass meine Vorschläge zum Datenschutz bei der Umsetzung des Vorhabens berücksichtigt werden.

9.15 Zentrales Datenschutzkonzept und Verfahrensbeschreibungen beim Stadtamt Bremen

Im Berichtsjahr wurden mir vom Stadtamt Bremen scheinbar mehrere unzureichende Verfahrensbeschreibungen zur Stellungnahme übergeben. Zum einen handelte es sich hier um die seit 2002 von mir geforderte Verfahrensbeschreibung zur Waffenverwaltung, zum anderen um Angaben zu Verfahren, die beim Bürger-Service-Center (BSC) genutzt werden.

Insgesamt musste ich feststellen, dass es keine übergreifende Dokumentation gibt, in der die allgemeinen Sicherheits- und Datenschutzmaßnahmen des Stadtamtes beschrieben sind. Hierzu zähle ich auch das BSC, da es technisch mit den Fachverfahren für das Meldewesen (MESO), Gewerbe (GewNeu/MIGEWA), Kfz-Zulassung (eKol/IKol), Führerschein, Fischereiangelegenheiten, Ausländer/Verpflichtungserklärungen und weiteren Anwendungen an das Stadtamt gebunden ist. Inhalt einer solchen Dokumentation sollten unter anderem die internen IT-Sicherheitsziele und Maßnahmen zu ihrer Umsetzung, die Beschreibung der Sicherheitsaspekte der Netzinfrastruktur sowie auch Sicherheitsmechanismen zur Zutritts-, Zugangs-, Verfügbarkeits- und Weitergabekontrolle sein.

Neben der Erstellung des allgemeinen Sicherheits- und Datenschutzkonzepts ist eine Anpassung der einzelnen Fachdatenschutzkonzepte für die Waffenverwaltung und die vom BSC genutzten Anwendungen erforderlich. Hier fehlt es beispielweise an der durchgängigen und vollständigen Beschreibung der Prozesse sowie an Angaben zur Zugriffskontrolle, zur Protokollierung und zur Administration.

Mehrfach habe ich die Erstellung der erforderlichen Datenschutzkonzepte für Stadtamt und BSC gefordert. Erst in der Sitzung des Rechtsausschusses im November des Berichtsjahres wurde von einem Vertreter des Innenressorts und vom Leiter des Stadtamts zugesagt, die spätestens seit 2003 überfällige Bestellung eines behördlichen Datenschutzbeauftragten vorzunehmen, wie aber auch mit Hilfe eines externen Unternehmens die Erstellung des Datenschutzkonzeptes zu beauftragen. Kurz vor Weihnachten 2005 ging bei mir eine Vorstudie „Unterstützung Datenschutzkonzeptorganisation Stadtamt“ ein. Hierzu habe ich Stellung genommen.

Im Februar fand die Kick-Off-Veranstaltung für die Erstellung der genannten Datenschutzkonzepte statt. Die Terminplanung sieht vor, dass die ersten Fachdatenschutzkonzepte sowie das allgemeine Rahmendatenschutzkonzept bis Ende April 2006 abgeschlossen sein sollen. Es bleibt zu hoffen, dass der zähe Fortgang der Erstellung der Datenschutzkonzepte und des Verfahrensverzeichnis in 2006 ein Ende finden wird.

9.16 Einführung eines neuen DV-Verfahrens bei der Meldebehörde

Bremen

Da das bisherige DV-Verfahren den melderechtlichen Anforderungen nicht mehr gerecht wurde, gelangt seit Ende des Berichtsjahres - wie bei zahlreichen anderen Meldebehörden in Deutschland - auch in Bremen das DV-Verfahren MESO (Meldebehördensoftware) zum Einsatz. Die Einführung des neuen Verfahrens erfolgt schrittweise, wobei die Verfahrensteile „Personalausweis- und Passregister“, „Lohnsteuer“ und „Wahlen“ erst bei weiteren Schritten implementiert werden sollen. Die Software enthält umfangreiche Programmkomponenten, deren Nutzung die Bearbeitung von Vorgängen im Bereich des Meldewesens erheblich vereinfachen soll.

Verbunden mit der Einführung sind jedoch auch erhebliche datenschutzrechtliche Fragestellungen, die vor der Inbetriebnahme eines derartigen Verfahrens geklärt werden müssen. Nachdem ich von der Meldebehörde über ihre Absicht, ein neues DV-Verfahren zu implementieren, unterrichtet und um eine datenschutzrechtliche Beratung gebeten worden war, hatte ich sie bereits im Frühjahr des vergangenen Jahres auf die zu klärenden Punkte aufmerksam gemacht. Um das vorgesehene DV-Verfahren beurteilen zu können, bat ich die Meldebehörde u. a., mir eine Verfahrensbeschreibung zum neuen Verfahren einschließlich Datensatz- und Datenbankbeschreibungen, Auflistungen von Mitteilungs- und Übermittlungsdiensten, Informationen zu eGovernment-Anwendungen, Informationen über die Berücksichtigung von Auskunftss- und Übermittlungssperren sowie ein Datenschutzkonzept mit den vorgesehenen technischen und organisatorischen Sicherungsmaßnahmen (insbesondere im Hinblick auf die vorhandenen Zugriffsmöglichkeiten, die vorgesehenen Datenübermittlungen und Protokollierungen) zukommen zu lassen. Zu meinem Bedauern habe ich hiervon bislang erst einen sehr kleinen Teil der Unterlagen erhalten, die ihrerseits dann wieder zahlreiche Fragen hinsichtlich der Datenverarbeitung mit dem Verfahren MESO aufwerfen. Eine Beurteilung des Verfahrens war mir somit bislang nicht möglich. Trotzdem wird MESO von der Meldebehörde eingesetzt. Möglicherweise bestehende datenschutzrechtliche Mängel konnten vor der Inbetriebnahme des Verfahrens nicht mehr behoben werden, was zu erheblichen Datenschutzverletzungen im laufenden Betrieb führen kann.

Ich habe der Meldebehörde noch einmal mitgeteilt, welche Informationen und Unterlagen von mir benötigt werden. Für den Fall, dass mir diese auch weiterhin nicht zur Verfügung gestellt werden, behalte ich mir eine formelle Beanstandung gegenüber dem Senator für Inneres und Sport ausdrücklich vor.

9.17 FundInfo über das Internet

Im September des Berichtsjahres hat das Fundamt des Stadtamtes die Internet-Anwendung FundInfo eingeführt. Dabei sind die Datenbestände bestehender Fundbüros im Land Bremen und zahlreicher Umlandgemeinden vernetzt und in einer zentralen Datenbank zusammengeführt worden. Der Bürger kann nun jederzeit von zu Hause über das Internet nach verlorenen Gegenständen suchen. Die Suche wird durch Angabe eines Suchgebietes, Kategorien von Gegenständen (z. B. Schlüssel, Ausweis, Fahrrad) und den Tag, seit dem der Gegenstand vermisst wird, eingegrenzt. Anschließend zeigt FundInfo eine Liste der Sucheinträge mit einer kurzen Beschreibung des Gegenstandes, dem Funddatum und -ort sowie das zuständige Fundbüro an. Wie bisher bleibt darüber hinaus die telefonische Auskunft oder das persönliche Aufsuchen des Fundbüros möglich.

Fundsachen wie Brieftaschen oder Mobiltelefone enthalten oft personenbezogene Daten bis hin zu sensiblen Daten des Betroffenen, z. B. einen Schwerbehindertenausweis, Rechnungen oder Fotos. Auch bei der Fundsachenverwaltung fallen personenbezogene Daten des Finders z. B. für Finderlohnansprüche und des Eigentümers der verlorenen Sachen an. Ich habe mich dafür eingesetzt, dass der Schutz der personenbezogenen Daten innerhalb der Datenbank und beim Zugriff über das Internet technisch und organisatorisch sichergestellt wird. Auch dürfen nicht mehr personenbezogene Daten als für die Fundsachenverwaltung erforderlich aufgenommen oder über FundInfo im Internet zugänglich sein. Die Einführung von FundInfo wurde von mir aus datenschutzrechtlicher Sicht begleitet. Zur Zeit steht noch die Erstellung einer Verfahrensbeschreibung nach § 8 Bremisches Datenschutzgesetz (BremDSG) aus.

9.18 Eingaben betreffend die Meldebehörde

Wiederholt erhielt ich im Berichtsjahr Eingaben von Bürgern, die die unzulässige Verarbeitung ihrer Daten durch die Einwohnermeldebehörde betrafen. Ein Bürger beklagte sich, dass die Meldebehörde Bremen für ihn eine Abmeldung von seinem Wohnsitz vollzogen habe, obgleich sich dieser nicht verändert hätte. Der Petent erklärte, dass die Abmeldung von Amts wegen vorgenommen worden sei, nachdem Nachbarn von ihm der Behörde mitgeteilt hätten, dass mein Petent verzogen sei. Gemäß § 21 Satz 1 bremisches Meldgesetz (BremMeldG) hat die Meldebehörde das Melderegister von Amts wegen fortzuschreiben, wenn sich gespeicherte Daten geändert haben oder wenn neue oder weitere Daten zu speichern sind. Wie die Meldebehörde bei meiner Prüfung bestätigte, war jedoch die notwendige Überprüfung der Angaben bedauerlicherweise unterblieben. Die Meldebehörde hätte die ihr zugeleiteten Informationen z. B. durch eine Befragung des Wohnungsgebers überprüfen müssen. Der festgestellte Sachverhalt wurde zum Anlass genommen, die zuständigen Mitarbeiter der Meldebehörde für die Problemlage zu sensibilisieren. Das Melderegister wurde nach § 10 BremMeldG korrigiert, wonach unrichtig gespeicherte Daten zu berichtigen sind.

In einem anderen Fall beklagte sich ein Bürger über die Erteilung von nicht zulässigen Auskünften zu seiner Person an Unternehmen der Privatwirtschaft. Die Auskünfte seien an die Firmen erteilt worden, obwohl die Meldebehörde Bremen nicht nach ihm, sondern nach einer anderen Person mit gleichem Namen gefragt worden sei. Um die Verwechslung zu vermeiden, hätte die Meldebehörde nur weitere Angaben zum Betroffenen, u. a. die ihr genannte frühere Anschrift, präziser berücksichtigen müssen, was nicht geschehen sei. Durch die Verwechslung wurden dem Petenten durch das Unternehmen der Privatwirtschaft äußerst sensible Daten bekannt, die für ihn sonst nicht zugänglich gewesen wären. Er erhielt u. a. Kenntnis von nicht bezahlten Rechnungen und laufenden Mahnverfahren. Gemäß § 32 Abs. 1 und 2 BremMeldG darf die Meldebehörde Auskünfte nur über einzelne bestimmte Einwohner erteilen. Dies bedeutet u. a., dass der Einwohner, zu dem eine Auskunft verlangt wird, vom Auskunftsuchenden so zu bestimmen ist, dass eine eindeutige Identifikation möglich wird. Eine Verwechslung der Person, zu der Auskunft erteilt wird, darf nicht vorkommen. Auf mein Anschreiben bestritt die Meldebehörde Bremen, bei der Erteilung der Auskünfte über den Petenten einen Fehler gemacht zu haben. Da der Straßename bei der Selektion der Person, über die beauskunftet wurde, Berücksichtigung fand und unter dem Straßennamen keine weitere Person gemeldet war, sei die bei der Erteilung solcher Auskünfte gebotene Sorgfalt berücksichtigt worden. Im Übrigen weise die Meldebehörde bei der Erteilung von Melderegisterauskünften die Auskunftsuchenden ausdrücklich darauf hin, dass keine Gewähr dafür übernommen werden kann, dass die ermittelte mit der tatsächlich gesuchten Person übereinstimmt.

Zu den Ausführungen der Meldebehörde Bremen wies ich darauf hin, dass gemäß § 7 BremMeldG die schutzwürdigen Belange der Betroffenen zu wahren sind. Übermittelt werden dürfen Daten nur zu der Person, zu der angefragt wurde; anderenfalls ist die Übermittlung unzulässig. Bestehen Zweifel, ob die aus dem Melderegister selektierten Daten der Person zuzuordnen sind, zu der angefragt wurde, ist die Übermittlung zu unterlassen. Der Hinweis an die Auskunftsuchenden, dass keine Gewähr dafür übernommen werden kann, dass die ermittelte Person mit der tatsächlich gesuchten Person

übereinstimmt, reicht zur Wahrung der schutzwürdigen Belange der Betroffenen nicht aus. Ich halte an meiner Auffassung fest, dass die Meldebehörde bei der Übermittlung der den Petenten betreffenden Daten die gebotene Sorgfalt unbeachtet ließ, und forderte diese nochmals auf, bei der Erteilung von Auskünften nach § 32 BremMeldG künftig sorgfältiger vorzugehen, ihr Verfahren bei der Auskunftserteilung im Hinblick auf die Wahrung der schutzwürdigen Belange der Betroffenen ggf. zu verbessern und mir dies entsprechend zu bestätigen. Die Bestätigung steht noch aus.

9.19 Einführung des ePasses

Seit dem 1. November 2005 wird in Deutschland der so genannte ePass ausgegeben. Der neue Reisepass ist mit einem elektronischen Speicherchip versehen, der ein Gesichtsbild des Passinhabers enthält. Von März 2007 an sollen auf dem Chip auch Fingerabdrücke gespeichert werden. Grundlage hierfür ist eine EU-Verordnung aus dem Jahr 2004, die nicht zuletzt nach den Anschlägen des 11. September 2001 auf Druck der USA verabschiedet worden ist. Interessant ist dies deshalb, weil in den USA bislang nicht einmal ein bundesweit einheitlicher Personalausweis existiert, den die Bürger mit sich führen müssen.

Für die Bremer Bürgerinnen und Bürger wird sich bei der Beantragung eines solchen Biometriepasses zunächst nichts ändern. Lediglich an das vorzulegende Lichtbild werden andere Anforderungen gestellt als bisher. Außerdem wird die Gebühr für das Dokument erhöht. Für einen normalen Reisepass zahlt man nun 59 € statt bisher 26 €.

Ich halte die Einführung biometrischer Pässe aus datenschutzrechtlicher Sicht für bedenklich. Die Speicherung biometrischer Merkmale in Ausweisdokumenten führt nicht automatisch auch zur Verbesserung der Sicherheit. Denn nicht die deutschen Bürgerinnen und Bürger sind vornehmlich das Sicherheitsrisiko. Solange daher nicht weltweit einheitliche Verfahren bei der Passvergabe gewährleistet sind, wird es keinen gravierenden Sicherheitszuwachs geben. Das gilt umso mehr, als in einigen Staaten bislang nicht einmal fälschungssichere Ausweispapiere ausgegeben werden. Außerdem existieren bisher keine international gültigen Regelungen, die gewährleisten, dass biometrische Daten deutscher Staatsbürger nicht in anderen Staaten in externen Datenbanken gespeichert werden. Ich bezweifle aus diesen Gründen die Geeignetheit und Erforderlichkeit der Einführung biometrischer Pässe.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beurteilt die Einführung biometrischer Ausweisdokumente kritisch. In ihrer EntschlieÙung vom 1. Juni 2005 (vgl. Ziff. 19.11 dieses Berichts) fordert die Konferenz, dass mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten erst begonnen wird, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Bis heute liegt jedoch ein umfassendes Sicherheitskonzept nicht vor. Außerdem fehlen im Passgesetz Regelungen zur strikten Zweckbindung der Daten.

9.20 Veröffentlichung von Daten von Beiratsmitgliedern und „Fachberatern“ im Internet

In einem Ortsamtsbereich wurden in Form einer „Stadtteilbroschüre“ im Internet personenbezogene Daten, unter anderem der Mitglieder der Beiräte und der Fachausschüsse, veröffentlicht. Die Veröffentlichung betraf dabei nicht nur die regulären Beiratsmitglieder, sondern auch die so genannten sachkundigen Bürger, die nur in nicht-öffentlichen Sitzungen der Fachausschüsse in Erscheinung treten. Einer dieser Bürger wandte sich an mich, da er mit der Veröffentlichung in dieser Form nicht einverstanden war.

Bei der Veröffentlichung im Internet handelt es sich rechtstechnisch um eine Übermittlung personenbezogener Daten, die nur zulässig ist, soweit der Betroffene eingewilligt hat oder Rechtsvorschriften die Veröffentlichung erlauben oder voraussetzen. Vorliegend fehlte es sowohl an einer Einwilligung der Betroffenen als auch an einer Rechtsvorschrift. Auf meinen Hinweis gegenüber dem Ortsamtsleiter werden die personenbezogenen Daten nunmehr nur mit Einwilligung der Betroffenen veröffentlicht. Bei den sachkundigen Bürgern werden selbst dann nur die Namen, nicht jedoch die Adresse und Telefonnummer oder E-Mail-Adresse wiedergegeben.