Datenschutzbericht

2009-2011

des behördlichen Datenschutzbeauftragten

Datenschutzbericht 2009-2011

1. Der Datenschutzbeauftragte der Stadt Gießen

Gemäß Beschluss der Stadtverordnetenversammlung der Universitätsstadt Gießen vom 30. Januar 1986 hat der/die behördliche Datenschutzbeauftragte den städtischen Gremien über seine/ihre Tätigkeit zu berichten.
Die Zusammenfassung der Berichte für die Jahre 2009-2011 erfolgt wie bereits in früheren Jahren aus prozessökonomischen Gründen. Auf die Schlussbemerkung wird verwiesen.

Die Berichterstattung hat sich an datenschutzrechtlichen Bestimmungen zu orientieren. Entsprechend erfolgt in dieser Berichterstattung eine Zusammenfassung wesentlicher Informationen aus den Jahren 2009-2011. Eine Darstellung personenbezogener oder sozial sensibler Daten erfolgt nicht. Auf die Arbeitspapiere des Datenschutzbeauftragten wird verwiesen.

1.1. Zur Person des behördlichen Datenschutzbeauftragten

Die Bestellung des Unterzeichners zum behördlichen Datenschutzbeauftragten erfolgte mit Wirkung vom 01.03.2009 durch den Magistrat. Die Bestellung von Herrn Wolfgang Panz zum stellvertretenden Datenschutzbeauftragten (Magistratsbeschluss vom 02.08.1999) ist nach wie vor gültig.

1.2. Ausgewählte Fort- und Weiterbildung des Datenschutzbeauftragten in den Jahren 2009-2011

- Teilnahme der Datenschutzbeauftragten/bzw. des Vertreters an dem Arbeitskreis der städt. Datenschutzbeauftragten der Hess. Städte über 50.000 Einwohner. Wie bereits seit 1990 tagten die städtischen Datenschutzbeauftragten der Hess. Städte über 50.000 Einwohner auch im Jahre 2009-2011 zweimal.

- Technikunterstützter Datenschutz - Einsatz von WEKA-Software

- Korruption und Datenschutz - Schulung in Bonn

- Teilnahme am Arbeitskreis Korruptionsprävention Mittelhessen

Es erfolgt darüber hinaus eine enge Zusammenarbeit mit dem Hessischen Datenschutzbeauftragten über regelmäßige schriftliche und mündliche Kommunikation.

1.3. Aufgaben und Stellung des behördlichen Datenschutzbeauftragten

Behördliche Datenschutzbeauftragte sind unmittelbar der Leitung der Behörde zu unterstellen. Dies trägt der besonderen Position des/der Datenschutzbeauftragten Rechnung und ermöglicht den direkten Kontakt zur Leitung der Behörde ohne Einhaltung eines sonstigen Dienstweges. Das Hessische Datenschutzgesetz benennt als Aufgaben der/des behördlichen Datenschutzbeauftragten insbesondere

- das Hinwirken auf die Einhaltung der Datenschutzvorschriften
- die Unterstützung der Behörde bei der Erstellung des Verfahrensverzeichnisses (§ 6 Abs. 1 HDSG)
- die Überprüfung der Vorabkontrolle bei Einsatz oder Änderung von Verfahren und der automatisierten Verarbeitung personenbezogener Daten (§ 7 Abs. 1 HDSG)
- die Unterrichtung der Beschäftigten über Vorschriften für den Datenschutz
- die Führung des Verfahrensverzeichnisses und die Bereithaltung zur Einsicht.

2. Datenschutz in der Verwaltung

In den Berichtsjahren 2009-2011 hat es Änderungen in den Rechtsgrundlagen gegeben. Die Änderungen wurden in der Aufgabenumsetzung berücksichtigt. Auf die Tätigkeitsberichte 2009 ff. des Hessischen Datenschutzbeauftragten und das Hessische Datenschutzgesetz wird verwiesen.

Die Vorgänge, mit denen sich der Unterzeichner als behördlicher Datenschutzbeauftragter der Stadt Gießen in den Berichtsjahren 2009-2011 befasste, sind zahlreich und hinsichtlich der datenschutzrechtlichen Fragestellungen vielseitig. Eine vollzählige Aufstellung erübrigt sich an dieser Stelle. Die Unterlagen über die bearbeiteten Vorgänge sind in den Arbeitspapieren des Datenschutzbeauftragten abgelegt.

Im Wesentlichen ist die Aufgabenwahrnehmung in 3 Kategorien zu unterteilen:

- **Anfragen**
- **Vorabkontrolle/Verfahrensverzeichnisse**
- **Mitarbeit in Projekten**

2.1. Anfragen

2.1.1. Anfragen aus den Fachämtern und/oder einzelner MitarbeiterInnen

Im Lauf der Berichtsjahre kam es zu zahlreichen datenschutzrechtlichen Anfragen aus den Fachämtern. Diese wurden in Einzelgesprächen oder mit entsprechendem Schriftverkehr abgearbeitet. Einige ausgewählte Vorgänge aus den Berichtsjahren 2009-2011 und die Ergebnisse der datenschutzrechtlichen Bewertungen werden nachfolgend aufgezeigt.

- **Zutrittskontrollsysteme/Videoüberwachungsanlagen**

Transponder

Unter Bezug auf die Regelungen des hessischen Datenschutzgesetzes der behördliche Datenschutzbeauftragte (§ 5 HDSG) hinsichtlich der Einrichtung des Zutrittskontrollsystems nachträglich eingeschaltet worden. Er steht seitdem in regelmäßigem Kontakt mit den Fachämtern (Amt für IT, Haupt- und Personalamt) sowie unter Berücksichtigung der entsprechenden Mitwirkungs- bzw. Mitbestimmungsrechte mit der Personalvertretung.

Der behördliche Datenschutzbeauftragte hat entsprechend auf die Beachtung und Umsetzung der datenschutzrechtlichen Bestimmungen, auf die Erstellung eines Verfahrensverzeichnisses und auf die entsprechende Dokumentation der notwendigen Unterlagen hingewiesen.

Die Erstellung des Verfahrensverzeichnisses wurde veranlasst und ist abgeschlossen. Das Verfahrensverzeichnis liegt dem behördlichen Datenschutzbeauftragte vor und wurde auf Vollständigkeit und inhaltliche Schlüssigkeit überprüft.

Das Verfahrensverzeichnis umfasst Regelungen zu den Zugangsberechtigungen bzw. der Zugangs- und Zutrittssicherung im Verfahren. Diese Regelungen beinhalten die Aspekte Zutrittskontrolle, Zugriffskontrolle, Datenverarbeitungskontrolle, Verantwortlichkeitskontrolle, Auftragskontrolle, Dokumentations- und Organisationskontrolle.

Die Einhaltung dieser Regelungen wird durch den behördlichen Datenschutzbeauftragten im späteren Geschäftsprozess kontrolliert und dokumentiert.

Videoüberwachungsanlagen

Der Hessische Datenschutzbeauftragte hat der Stadt Gießen im Januar 2009 folgende Hinweise zur Videoüberwachung an der Außenfassade zugeleitet:

1. *Eine Modifizierung der vorgesehenen Einstellung der Kameras an der Außenfassade hat zu erfolgen.*

2. *Ein Überblick über die Fassade (max.1- 1,5 m) und eines Teils der Gehwege wird als ausreichend betrachtet.*

3. *Eine Aufzeichnung soll auf ein begrenztes Zeitfenster (18:00 Uhr bis 06:00 Uhr) beschränkt werden.*

4. *Die Aufzeichnungen sind frühzeitig (nach ca. 10 bis max. 30 Tagen) zu löschen.*

5. *Eine Dienstvereinbarung ist zu erstellen.*

Die Hinweise zu Punkt 1. und 2. wurden bereits umgesetzt. Darüber hinaus sind nach wie vor Abstimmungen (z. B. die Möglichkeit der Umsetzung einer technischen Lösung von IT-Schnittstellen zum internen Netzwerk) erforderlich. Zur vorgesehenen Aufzeichnung (Punkt 3.) sieht der Hessische Datenschutzbeauftragte weiterhin das Problem, dass z. B. bei Abendveranstaltungen in dem vorgesehenen Zeitfenster eine Lösung gefunden werden muss, die den Besuchern den unbeobachteten Zugang zum Rathaus ermöglicht. Dafür sind Regelungen zu vereinbaren, welche die Anforderungen des Datenschutzrechtes und den dynamischen Charakter der Rechtssprechung berücksichtigen. In diesen wird sich eine Festlegung finden, wonach zu Punkt 4. eine Aufzeichnung längstens für 10 Tage vorgesehen ist.

Entsprechend hat sich die Stadt dazu entschlossen, die Festlegungen über Dienstvereinbarungen abzubilden. Darin sind die Anforderungen aus Sicht der Stadt Gießen gegenüber den möglichen Schutzbelangen der von der Überwachung Betroffenen abzuwägen. Der hessische Datenschutzbeauftragte hat daher den Unterzeichner gebeten, regelmäßig über die beabsichtigten und umgesetzten Maßnahmen zur Videoüberwachung der Außenfassade zu berichten. Hierzu gehört auch die Erstellung neuer Verfahrensverzeichnisse sowie die Darstellung technischen und organisatorischen Maßnahmen (§ 10 HDSG).

Die Videoüberwachung in der Tiefgarage ist bereits in Betrieb. Die technischen und organisatorischen Maßnahmen wurden mit dem Unterzeichner als behördlichem Datenschutzbeauftragten und dem HDSB weitestgehend abgestimmt.

Den vorgebrachten Empfehlungen wurde gefolgt. So ist z. B. der Zugriff auf die in einem separaten Raum untergebrachte, autonome Datenspeicherung passwortgeschützt nur dem behördlichen Datenschutzbeauftragten möglich. Eine regelmäßige Überprüfung der Aufzeichnungen erfolgt durch den behördlichen Datenschutzbeauftragten (1 x wöchentlich). Die Aufzeichnungen werden nach 10 Tagen gelöscht.

Zurzeit befindet sich der Entwurf einer Dienstvereinbarung zum Einsatz von (Zutrittskontrollsystemen und) Videoüberwachungsanlagen im Geschäftsgang der zu beteiligenden Fachämter (Haupt- und Personalamt, Amt für IT, Revisionsamt/Datenschutzbeauftragter).

- **Migration**

Zur Feststellung des Anteils von Beschäftigten/Bewerbern mit Migrationshintergrund sowie der interkulturellen Kompetenz von Beschäftigten/Bewerbern soll eine Erhebung bei der Universitätsstadt Gießen erfolgen. Erhebungsgrundlage sollen nach Aussage der Integrationsbeauftragten die Regelungen der Integrationskonzeption (Hessen: Leitlinien zur Integration 2007) sein.

Es wurde eine vorangehende, datenschutzrechtliche Stellungnahme angefragt (Auszug):

- Datenschutzrechtlich ist zu beurteilen, welche Zielsetzungen mit der geplanten Erhebung und Verarbeitung verbunden werden und wie diese Ziele mit datenschutzrechtlichen Anforderungen harmonisiert werden können. Insofern hat eine ausreichende Abwägung der notwendigen datenschutzrechtlichen Beschränkungen bei der Erhebung und Verarbeitung von Informationen über die ethnische Zugehörigkeit mit der für notwendig erachteten Erfassung und Auswertung dieser Informationen für bestimmte Zwecke zu erfolgen.

- Daten zur ethnischen Herkunft sind besonders schutzwürdige personenbezogene Daten. Datenschutzrechtlich ist das Grundrecht auf informationelle Selbstbestimmung betroffen. Hier ist es von Bedeutung, ob die Erhebung der Daten zur Erfüllung einer gesetzlichen Aufgabe oder für einen anderen, legitimen Zweck erforderlich ist und die schutzwürdigen Belange der Betroffenen nicht unangemessen beeinträchtigt werden.

- Generell gilt, dass konkrete Fragen nach einem Migrationshintergrund und eine personenbezogenen Erfassung der Herkunft rechtlich nicht zulässig sind. D. h. Daten können nur entweder auf rechtlicher Grundlage oder freiwillig im Einzelfall (dies bedeutet, dass eine Einwilligung zur Verarbeitung durch die Betroffenen erforderlich ist) erhoben werden. Diese Voraussetzungen existieren in dem genannten Sachverhalt (noch) nicht. Es existiert insofern keine bereichsspezifische Handhabe für die hier vorgesehene, verpflichtende Erhebung des Migrationshintergrundes („Ethnic Monitoring"). Aussagen über den Migrationshintergrund der Beschäftigten im öD sind des Weiteren auch im bundesweiten Vergleich nur partiell möglich und beruhen dann i. d. R. auf freiwilliger Auskunft. Insofern sind ethnische Erhebungen keine durchgängige Praxis.

- Die sehr allgemein formulierten Anforderungen an die Erhebung sind vor diesem Hintergrund nicht ausreichend und führen zu datenschutzrechtlichen Bedenken. Besonders zu betonen ist hierbei, dass es auch dem Schutz der Betroffenen dient, zu verhindern, dass unbeabsichtigte Schlussfolgerungen aus den erhobenen Daten gezogen werden.

- Eine sorgfältige Vorbereitung der vorgesehenen Erhebung ist deshalb datenschutzrechtlich erforderlich. Die Erhebungsmerkmale sind zu konkretisieren. Eine individuelle Einwilligung der Beschäftigten, d.h. eine Freiwilligkeit der Angaben ist vorauszusetzen. Die Auswertung hat anonymisiert zu erfolgen. Rückschlüsse auf Personen sind auszuschließen. Die vorgesehene Bevorratung der Daten zur Generierung von Aussagen und zur Evaluierung der Erkenntnisse ist nur unter bestimmten, festzulegenden Voraussetzungen zulässig.

Die geplante Erhebung und die konzeptionell beabsichtigte Bevorratung der Daten sind zusammengefasst in dieser Form - auch aus Sicht des Hessischen Datenschutzbeauftragten - datenschutzrechtlich nicht zulässig.

- **Live-Übertragung von Sitzungen**

Es handelt sich bei einer vorgesehenen Live-Übertragung öffentlicher Sitzungen (Ausschüsse und Stadtverordnetenversammlung) um die Übermittlung personenbezogener Daten an eine Vielzahl unbestimmter Personen. Hier bestehen bezüglich der vorherigen Zustimmung der Betroffenen (Stadträte/Bedienstete/Zuhörer), einer technischen Umsetzung sowie zur Beteiligung des Personalrates zu klärende Fragestellungen.

Der Hessische Datenschutzbeauftragten wurde um eine Beurteilung aus dessen Sicht gebeten. Dies erfolgte vor dem Hintergrund der Tatsache, dass solche Sachverhalte zunehmend in den Focus einer breiteren Öffentlichkeit treten und damit überregionale datenschutzrechtliche Relevanz haben.

Der HDSB vertritt nachfolgende Auffassung (Zitat):

„…Nach § 52 Abs.1 Hessische Gemeindeordnung (HGO) sind die Sitzungen der Gemeindevertretung grundsätzlich öffentlich. Nach h. M. bedeutet Öffentlichkeit i. S. dieser Vorschriften, dass jeder die Möglichkeit der Anwesenheit an den Sitzungen hat. Unbeteiligte können jederzeit den Sitzungsraum betreten, anwesend sein und den Sitzungsraum wieder verlassen.

Ein Recht zu Ton bzw. Bildaufnahmen wird von diesem Öffentlichkeitsprinzip nicht gedeckt. Die Gemeinde- bzw. Kreistagsvertreter müssen es danach nur hinnehmen, dass Zuhörer an den Sitzungen teilnehmen, sich eventuell Notizen machen und danach über die Sitzungen in der Presse berichtet wird. Schon zur Fertigung von Tonaufzeichnungen hat das Bundesverwaltungsgericht entschieden, dass das Recht des Gemeinderatsmitglieds auf freie Rede durch die Aufzeichnung auf Tonband empfindlich tangiert werden könne. Diese Bedenken bestehen bei einer Übertragung der Sitzungen ins Internet in erhöhtem Maße. Nach meiner Auffassung kann man die Internetübertragung auch nicht auf die ausdrückliche Einwilligung aller Gemeindevertretungsmitglieder stützen. Der Entscheidungsdruck auf einzelne Mitglieder kann unter Umständen so groß sein, dass von einer freiwilligen Einwilligung i. S. v. § 7 Abs.1 Nr. 3 Hessisches Datenschutzgesetz (HDSG) nicht mehr die Rede sein kann. Ich halte deshalb eine Übertragung der Sitzungen ins Internet nicht für zulässig. Hinzu kommt aus meiner Sicht noch folgende Überlegung. Öffnet man die Öffentlichkeit der kommunalen Vertretungskörperschaften in Richtung Internet, entsteht ein Druck, die bisherige Öffentlichkeit stärker einzuschränken, um damit nicht ins Internet zu gelangen. Die Gemeindevertretungsbeschlüsse werden dadurch fehleranfälliger. Die virtuelle sollte die faktische Wirklichkeit nicht verdrängen…".

Neben den Ausführungen des Hessischen Datenschutzbeauftragten waren aus Sicht des behördlichen Datenschutzbeauftragten keine zusätzlichen Anmerkungen zu machen.

- **Nutzung der IT durch nichtstädtische Bedienstete**

Die Anfrage bezog sich auf die Frage zur Nutzung von städtischem Eigentum (hier: insbesondere IT) durch nicht städtische Bedienstete. Im Rahmen einer internen Besprechung wurden zwischen dem Amt für IT und dem behördlichen Datenschutzbeauftragten zunächst die relevanten Fragestellungen herausgearbeitet. Die ersten Einschätzungen aus datenschutzrechtlicher Sicht sind durch den Unterzeichner mündlich bzw. schriftlich und in verschiedenen Sitzungsterminen an die entsprechende Organisationseinheit weitergeleitet worden. Darüber hinaus wurde im Nachgang der Hessische Datenschutzbeauftragte um eine rechtliche und technische Würdigung der seitens der Stadt vorgesehenen Maßnahmen aus übergeordneter Sicht gebeten (Zitat):

" Der von Ihnen geschilderte Sachverhalt beschreibt eine Anforderung, die in ähnlicher Ausprägung derzeit in vielen Kommunen an die IT gestellt wird. Dabei gibt es eine technische und eine korrespondierende rechtliche Sicht.

a) technische Sicht

Die in den Unterlagen als Variante 3 beschriebene technische Lösung ist im Prinzip geeignet, die datenschutzrechtlichen Anforderungen zu erfüllen. Sie stellt allerdings hohe Anforderungen an die richtige Administration, insbesondere soweit es die Vergabe und Kontrolle von Zugriffsrechten betrifft.

Da nach den Unterlagen nur städtische Computer genutzt werden, was in dem Konzept wichtig ist, ergeben sich daraus auch Anforderungen an die Konfiguration dieser Computer. Insbesondere müssen folgende Punkte erfüllt sein:

- Die (nicht städtischen) Bediensteten dürfen auf dem Computer keine Administratorrechte haben. Außer in begründeten Ausnahmefällen dürfen sie auch keine Hauptbenutzer sein.

- Die Boot-Reihenfolge im BIOS muss sicherstellen, dass ein Booten von externen Datenträgern (USB-Stick, CD, …) nicht möglich ist. Diese Einstellung muss durch ein ausreichend komplexes BIOS-Passwort geschützt sein.

- Die USB-Schnittstellen muss so gesichert sein, dass nur zugelassene USB-Geräte genutzt werden können.

b) rechtliche Sicht

Von den aufgeführten Personengruppen sind einige funktional so nahe an der Verwaltung, dass die Stadt Gießen einen Überblick über die Nutzer hätte und diese oft auch öffentliche Aufgaben wahrnehmen. Bei diesen Gruppen handelt es sich beispielsweise um

- Stadtverordnete
- Mitarbeiter von Fraktionen
- Ausländerbeirat
- Mitarbeiter von städtischen Gesellschaften
- freiwillige Feuerwehren

Für diese Gruppen ist die beschriebene Nutzung möglich. Andere Gruppen sind für die Stadt Gießen eher anonym, so dass regelmäßig kein Zugriff zugelassen sein sollte. Dies betrifft beispielsweise - Mitglieder von Parteien (Ausnahmen für einzelne Mitglieder s.o.) - ehrenamtlich Tätige, soweit nicht der Bezug zur Stadt gegeben ist - Mitglieder von Vereinen, soweit nicht der Bezug zur Stadt gegeben ist. Vor einer Freischaltung ist immer eine entsprechende Prüfung erforderlich."

Es war damit auch aus Sicht des Unterzeichners als behördlichem Datenschutzbeauftragten zutreffend festzustellen, dass der HDSB die von der Stadt geplante Verfahrensweise unter den genannten Voraussetzungen als geeignet ansieht. Er folgert ergänzend, dass hierfür neben einer klar differenzierbaren Nutzerstruktur über Unterscheidungsmerkmale bei den Nutzern z. B. Zugriffe ins städtische Netz nur als geordneter Zugriff mit Einschränkungen und/oder minimalen Rechten erfolgen dürfen.

Ein Datenzugriff ist demnach nur zulässig, wenn diese Daten für die Aufgabenwahrnehmung erforderlich sind. Der Sachverhalt befindet sich aktuell in der Umsetzung.

- **Einsatz von USB-Sticks bei der Feuerwehr/Florix**

Die Feuerwehr Gießen (Berufsfeuerwehr und die Freiwilligen Feuerwehren) haben auf die Webanwendung/Fachverfahren ZMS/Florix umgestellt, wodurch sich die datenschutzrechtliche Problematik ergab, ob die die Funktionsträger (z.B. Amtsleitung, Wachabteilungsleiter, Florixbeauftragte, Wehrführer, Gerätewarte, Jugendwarte etc..) über ihren privaten PC zu Hause auf diese Anwendung zugreifen können sollten.

Der Zugang soll über ein Browserzertifikat und Benutzer Authentifizierung geregelt werden.

Für diese sog. "private" Nutzung gibt es, speziell für diese Anwendung, einen kopiergeschützten USB-Stick, der diesen Zugang zum ZMS/Florix gesichert ermöglicht.

An den behördlichen Datenschutzbeauftragten wurde die Frage gestellt, ob im Bezug auf den Datenschutz (privater PC) diese speziellen USB-Sticks in den Geschäftsgang (Beschaffung) gebracht werden können.

Nach Abstimmung mit dem HDSB, dem diese angesprochene USB-Lösung bekannt ist, konnte diese als (Übergangs-)Lösung akzeptiert werden, wenn dem Funktionsträger kein Dienst-PC zur Verfügung gestellt werden kann (siehe 38. Tätigkeitsbericht des HDSB, Ziff 5.7.1) Eine erweiterte Lösung, wie sie im Tätigkeitsbericht angesprochen wurde, ist noch nicht verfügbar.

Es ergaben sich keine datenschutzrechtlichen Bedenken, wenn die Stadt Gießen eine entsprechende Beschaffung für den in der Anfrage genannten Personenkreis vornimmt.

- **LA 21 - sichtbare E-Mail-Verteiler**

Dem behördlichen Datenschutzbeauftragten wurde bekannt gemacht, dass es in der LA21 üblich ist, dass Email-Verteiler sichtbar sind, z.B. beim Einladungsversand zu Gruppensitzungen. Dort stehen die Email-Adressen von aktiv Teilnehmenden im "An"-Feld, die von "stillen Teilnehmenden", d.h. am Thema Interessierten, die aber keine Zeit haben sich aktiv zu engagieren, in "cc".

Dem behördlichen Datenschutzbeauftragten wurde die Frage gestellt, ob diese Vorgehensweise datenschutzrechtlich weiter so handhaben wäre und ob diese offenen Verteiler auch noch vertretbar seien, wenn eine Informations-E-Mail an alle LA21-Beteiligten (aktive und stille) versendet würde.

Darüber hinaus würden im Rahmen des Kunstspectaculums nicht in der LA21-organisierte Künstler und Partner angeschrieben. Hier ging der Fragesteller davon aus, dass spätestens hier mit einem bcc-Verteiler gearbeitet werden müsse.

Aus datenschutzrechtlicher Sicht wurden sichtbare E-Mail-Verteiler dann als unproblematisch beurteilt, wenn beispielsweise verschiedene Behörden unterrichtet werden; hier also lediglich verschiedene Amtsträger erkennbar sind.

Bei dem Projekt LA21 wurde insofern eine Einladungsliste an die aktiven Teilnehmer im sichtbaren Adressfeld für zulässig gehalten. Alle anderen Empfänger von Mails sollten grundsätzlich unter bcc gesetzt werden.

- **Bereitbandinternet**

Im Rahmen der Ausgestaltung der städtischen Breitband-Internetversorgung wurde ein Fragebogen entwickelt, der dem Datenschutzbeauftragten nachträglich zur datenschutzrechtlichen Bewertung zugeleitet wurde. Dieser Fragebogen wurde jedoch vorab an die Haushalte ausgeliefert (im Wege der Zustellung durch die Sonntagszeitung). Eine Änderung des Fragebogens durch Eingaben des behördlichen Datenschutzbeauftragten war somit nicht mehr möglich.

Aus datenschutzrechtlicher Sicht wurden ungeachtet dessen gegen den Fragebogen keine grundsätzlichen Vorbehalte geäußert, da eine Antwortpflicht nicht zwingend vorgeben war. Dies hätte im Anschreiben an die Adressaten aber klarer formuliert werden müssen. Zum Fragebogen war anzumerken, dass die Option der anonymisierten Weitergabe (natürlich) auch die Telefonnummer und die E-Mail-Adresse auslassen muss; hier wäre eine Klarstellung nötig gewesen. Es dürfte dann nur die Straße weitergegeben werden.

Der potentielle Anbieter benötigt die Informationen für seine Planung, um seine Kosten kalkulieren und Wirtschaftlichkeitsbetrachtungen durchführen zu können. Es wurde hierzu plausibel dargelegt, dass die Hausnummer für Planungen wichtig sein kann. Deshalb wurde es datenschutzrechtlich akzeptiert, wenn die Hausnummer ebenfalls weitergegeben wird. Da die Stadt Gießen darauf verzichtet, handelt es sich tatsächlich um eine weitgehend anonymisierte Weitergabe. Den zuständigen Fachämtern wurde empfohlen, bei der Auswertung und Speicherung der Daten besondere Sensibilität zu wahren. Mit den genannten Änderungen wurde der Fragebogen auch aus Sicht des HDSB als datenschutzrechtlich nicht problematisch beurteilt.

- **Abbildung der Empfänger freiwilliger Leistungen in den Unterlagen zur Haushaltskonsolidierung der Stadt**

Im Rahmen der Haushaltskonsolidierungen wurden in Listen "postengenau" sämtliche Freiwillige Leistungen der Stadt Gießen erfasst. Dabei wurde auch dokumentiert, an welchen Empfänger die Freiwillige Leistung gezahlt wurde. Diese Liste sollte nun - gem. Beschluss der Stadtverordnetenversammlung - der Stadtverordnetenversammlung vorgelegt werden. Die Diskussion dieses Tagesordnungspunktes war für den öffentlichen Teil der Sitzung vorgesehen.

An den Datenschutzbeauftragten erging die Bitte zur Beantwortung folgender Fragen:

„1. Bestehen aus datenschutzrechtlicher Sicht grundsätzliche Bedenken gegen die Vorlage der v. g. Liste?

2. Verletzten bestimmte Angaben zu Empfängern Freiwilliger Leistungen datenschutzrechtlich schutzwürdige Belange? Wenn ja, bei welchen Positionen ist dies der Fall?"

Aus datenschutzrechtlicher Sicht erfolgte nachfolgende Stellungnahme:

„1. Grundsätzliche Bedenken aus datenschutzrechtlicher Sicht werden nicht gesehen.

2. In der Aufstellung sind zum Teil konkrete Namen von Empfängern (s. verschiedene lfd. Nr.) genannt. Dies wäre zu anonymisieren. Was die Angaben insgesamt anbelangt, stehen hier aufgaben- bzw. funktionsbezogenen Daten im Vordergrund. Die in der Liste aufgeführten Namen der MitarbeiterInnen stehen im Zusammenhang mit der Funktion und dem Gegenstand der Informationen. Als "Amtsträger" ist eine öffentliche Nennung daher zumutbar. Diese Stellungnahme wurde mit dem Hessischen Datenschutzbeauftragten abgestimmt."

- **DS an der Außenfassade sowie im Innenbereich/Ausländerbehörde und der Bibliothek**

Es wurde die Anbringung von Blendbändern/Sichtschutz an den außen liegenden Fenstern im Erdgeschoss durch den behördlichen Datenschutzbeauftragten gefordert und entsprechend umgesetzt. Für den Bereich der PC mit Internetzugang in der Bibliothek wurde ebenfalls auf Anforderung durch den behördlichen Datenschutzbeauftragten ein Sichtschutz an den Fenstern zum Flur angebracht.

- **Einrichtung von Heimarbeitsplätzen/mobile Arbeitsplätze**

In den Berichtsjahren wurden für verschiedene MitarbeiterInnen alternierende Telearbeitsplätze eingerichtet. Mit den Bediensteten wurden bezüglich der Einhaltung der Datengeheimnisse im häuslichen Bereich entsprechende Vereinbarungen getroffen. Durch den Datenschutzbeauftragten erfolgte vorab ein Hausbesuch. Hierbei wurde ebenfalls festgelegt, dass die mit der Bediensteten geschlossene Vereinbarung aus datenschutzrechtlicher Sicht konsequent einzuhalten ist.

Häusliche und damit datenschutzrechtlich relevante Änderungen sind entsprechend mitzuteilen. Eine Überprüfung der häuslichen Verhältnisse ist dem behördlichen Datenschutzbeauftragten möglich. Die Vertragsunterlagen wurden mit dem Haupt- und Personalamt abgestimmt.

- **Prüfung und Genehmigung der Zugriffsberechtigung einschl. des Verfahrensablaufes nach § 31 Hess. Meldegesetz (HMG) für Bedienstete der Stadtverwaltung Gießen (mehrere Vorgänge)**

- **Melderegisterauskünfte nach § 35 Hess. Meldegesetz (HMG) in besonderen Fällen (mehrere Vorgänge)**

- **Forschungsvorhaben z. B. der infas - Institut für angewandte Sozialwissenschaften GmbH, Bonn sowie anderer Forschungsinstitutionen (mehrere Vorgänge)**

In diesen zahlreichen Sachverhalten wurde nach Prüfung durch den behördlichen Datenschutzbeauftragten jeweils für den Einzelfall eine entsprechende Genehmigung bzw. Versagung erteilt. Die Unterlagen sind in den Arbeitspapieren des behördlichen Datenschutzbeauftragten abgelegt.

2.1.2. Anfragen aus dem externen Bereich (BürgerInnen/Institutionen)

Der Datenschutzbeauftragte der Universitätsstadt Gießen ist zuständig für die Belange des Datenschutzes der Stadtverwaltung. Die Bearbeitung von Anfragen aus dem privaten Bereich (BürgerInnen/Private Institutionen) kann nach diesem Verständnis nicht dem Aufgabenbereich zugeordnet werden. Ungeachtet dessen wurde aus Gründen der Bürgerorientierung verschiedene Einzelanfragen bei Telefonaten bzw. Beratungsgesprächen bearbeitet.

Beispielhaft seien an dieser Stelle genannt:

- Videoüberwachung im privaten Bereich (z. B. im Gaststättenbereich oder bei Supermärkten)

- Anfragen z. B. zur datenschutzrechtlichen Würdigung der Darstellung von Informationen aus dem MAG in der Presse oder zur öffentlichen Diskussion von Eigentumsverhältnissen von ehrenamtlich Tätigen bei Grundstücksangelegenheiten

- Bismarck-Turm Giessen

Die Anfragen wurden in Einzelgesprächen beurteilt und unter Hinweis auf die datenschutzrechtliche Zuständigkeit (z. B. nach dem BDSG) bzw. zur Beantwortung entsprechend weitergeleitet.

2.2. Vorabkontrolle/Verfahrensverzeichnisse nach §§ 6 und 7 HDSG

Die erforderlichen Sachverhalte werden im Zuge der zur Verfügung stehenden Ressourcen abgearbeitet. Auf die Schlussbemerkung wird verwiesen.

2.3. Mitarbeit an Projekten

Der Datenschutzbeauftragte wurde in den Berichtsjahren an verschiedenen Projekten der Stadtverwaltung beteiligt. Beispielhaft sollen hier die Stellungnahmen und Aussagen zur Mitarbeiterbefragung und der Verkehrsmessung/Telefon aufgezeigt werden.

2.3.1. Mitarbeiterbefragung

Im Rahmen der Zuständigkeit wurde der behördliche Datenschutzbeauftragte bei der vorgesehenen Mitarbeiterbefragung eingebunden. Es wurde die nachfolgende Stellungnahme verfasst (Auszug).

„Die bei der Universitätsstadt Gießen vorgesehene Mitarbeiterbefragung fragt nach dem ersten Eindruck der Unterlagen subjektive Einschätzungen über das Arbeitsumfeld ab. Dementsprechend enthält der Befragungsbogen konkrete Fragen zur Zufriedenheit (Betriebsklima der jeweiligen Organisationseinheit, Motivation, Arbeitsbelastung), Bewertungen von Entscheidungs- und Kommunikationsabläufen oder zum Führungs- und Vorgesetztenverhalten, etwa zur Einschätzung der fachlichen und sozialen Kompetenz von Vorgesetzten.

Die vorgesehene Mitarbeiterbefragung baut aussagegemäß im Wesentlichen auf den Erfahrungen und Grundlagen der beim Landkreis Gießen durchgeführten Verfahren auf.

Nach einer ersten, eigenen Beurteilung wurden dem HDSB die entsprechenden Unterlagen zu dessen Bewertung vorgelegt. Von diesem wird dann keine datenschutzrechtliche Problematik gesehen, wenn eine Beachtung der in den Basisunterlagen des Landkreises Gießen formulierten und empfohlenen Verfahrensschritte auch in dem bei der Universitätsstadt Gießen vorgesehen Verfahren (§§ 2 ff., 14, 16, 33 und 34 HDSG) erfolgt."

Zusammengefasst war demzufolge zur Ausgestaltung der Mitarbeiterbefragung bei der Universitätsstadt Gießen datenschutzrechtlich auf die folgenden Punkte hinzuweisen:

- Die Mitarbeiterbefragung muss anonym durchgeführt werden.
- Eine nachträgliche Zuordnung der Antworten zu den einzelnen Mitarbeitern hat zu unterbleiben.

  Einer besonderen Prüfung bedürfen insoweit die von den Teilnehmern in der Regel eingeforderten „statistischen Angaben". Werden hier wie beabsichtigt z. B. Angaben des konkreten Tätigkeitsfeldes, einer Vollzeit- oder Teilzeitbeschäftigung, des Geschlechts und des Lebensalters gefordert, besteht die Möglichkeit, teilnehmende Mitarbeiter durch eine Kombination dieser Angaben zu identifizieren. Ähnliche Schwierigkeiten ergeben sich, wenn eine Auswertung auch bezogen auf kleine Organisationseinheiten vorgesehen ist. Hierdurch könnte die zugesagte anonymisierte Auswertung ebenfalls in Frage gestellt werden.

  Dieses Problem lässt sich durch eine entsprechende Gruppengröße und eine Zusammenfassung der Daten bei der Auswertung lösen.

- Die Mitarbeiterbefragung ist nur auf freiwilliger Basis zulässig. Auch wegen der abgefragten subjektiven Einschätzungen und Bewertungen können mangels Rechtsgrundlage Mitarbeiter nicht zur Teilnahme verpflichtet werden.

- Wesentliche Bedeutung kommt einer vorherigen umfassenden Aufklärung und Information der MitarbeiterInnen zu. Der Hinweis auf die Freiwilligkeit ist in den Fragebögen selbst aufzunehmen und sollte drucktechnisch hervorgehoben werden. Die Information der Mitarbeiter alleine in einer Hausmitteilung oder über das hauseigene Intranet ist nicht ausreichend. Die MitarbeiterInnen sind über den Ablauf, den Gegenstand und den Zweck der Befragung und darüber, durch wen und für wen die Daten erhoben und verarbeitet werden, zu informieren. Auch sollten die Beschäftigten darüber aufgeklärt werden, welche Auswertungen konkret vorgesehen sind.

2.3.2. Verkehrsmessung/Telefon

Es wurde eine datenschutzrechtliche Stellungnahme zur Messung des Telefonverkehrsaufkommens in der Stadtverwaltung Gießen erbeten.

Diese Messung soll zum einen die Grundlage bilden zur Fragestellung, ob die Universitätsstadt Gießen an dem bundesweiten Behördenrufnummern-Projekt D 115 teilnimmt. Damit sollen den Anrufer/innen der Weg zum Ansprechpartner für ihr spezielles Anliegen erleichtert werden. Das dahinter liegende Service-Center soll kompetent und abschließend Auskunft geben können. Ansonsten sollen die Anrufer/innen zu den zuständigen Stellen und Organisationseinheiten weitergeleitet werden.

Dieser neue BürgerInnenservice soll mit den oben genannten Zielsetzungen die Voraussetzungen schaffen, dass eine nach einheitlichen Kriterien aufgebaute Dienstleistungserbringung für die Bürgerinnen und Bürger sichergestellt wird.
Ein dazu relevanter Ansatzpunkt ist die generelle telefonische Erreichbarkeit der Verwaltung. Hier liegt der Focus auf der **Analyse der eingehenden Anrufe**. Untersucht werden sollten die telefonische Erreichbarkeit der Ämter und Organisationseinheiten insgesamt (Servicelevel), die Messung des Anrufaufkommens (Anrufverteilung) und die Ermittlung der Zahl der Anrufer, welche eine Weitervermittlung über die 306-0-Rufnummer wünschen.

Zusätzliche Erkenntnisse sollten über die perspektivische Ausrichtung der Organisation, z. B. zu der transparenten Ablauforganisation, einer schnelleren Abwicklung der Anliegen und einer effizienteren Aufgabenerfüllung zur Optimierung der telefonischen Erreichbarkeit gewonnen werden.

Im Zusammenhang mit diesem Projekt wurden nachfolgend die wesentlichen, datenschutzrechtlichen Empfehlungen an die entsprechende Organisationseinheit/- Projektgruppe verfasst:

- „Im Rahmen des Projektes sollte die Analyse des Telefonaufkommens für noch zu bildende Cluster einschließlich einer gruppenbezogenen - nicht einzelfallbezogenen - Auswertung des Telefonaufkommens, der Dauer der Gespräche (nicht der Inhalte) sowie die Dauer bis zur Herstellung einer Verbindung vorgesehen werden.

- Ein Cluster sollte hierbei zu jeder Zeit eine bestimmte Anzahl von Nebenstellen-Rufnummern beinhalten, da aussagegemäß die gezielt angerufenen Nebenstellen registriert werden sollen. Werden wie beabsichtigt max. 20 Ämter und Abteilungen zusammengefasst, sollte ausgeschlossen werden, dass Leistungs- und Verhaltenskontrollmöglichkeiten einzelner Mitarbeiter/innen möglich sind.

- Die Daten sollten gruppenbezogen so aufbereitet werden, dass erstens kein Mitarbeiter/innenbezug (mehr) hergestellt werden kann (auch nicht bei kleineren Messgruppen), wobei die Verbindungsdaten hinsichtlich Dauer des Telefonats summiert und graphisch aufbereitet werden. Einheiten mit einer Beschäftigtenanzahl < 10 Mitarbeiter/innen sollten daher nicht als eigene Einheit erfasst werden.

- Eine Speicherung der eingehenden Rufnummern darf nicht erfolgen. Eine Messung/Kontrolle des Anrufverhaltens der Mitarbeiter/innen ist nicht zulässig; sie ist jedoch bei Einhaltung der Vorgabe, dass lediglich die eingehenden Anrufe erfasst werden, auszuschließen. Eine Erhebung der Rufnummern der Anrufenden erfolgt nicht. Die Rohdaten werden der Universitätsstadt Gießen nicht zur Verfügung gestellt.

- Es sind sinnvolle Messgruppen zu bilden (zu bestimmende Nebenstellen), um den Anteil der Vermittlung zu den gewünschten Ansprechpartner herauszuarbeiten. Dies erfolgt hinsichtlich der **eingehenden Anrufe** auf der Ebene ganzer Ämter und Abteilungen, so dass keinerlei Rückschlüsse auf das Telefonverhalten einzelner Personen erfolgen können.

- Es ist in der Folge sicherzustellen, dass eine Weitergabe der Daten den datenschutzrechtlichen Vorgaben im Sinne der Vorschriften des HDSG entspricht. D. h. nach vorangehender Beschlusslage werden intern (s. u.: Weitergabekontrolle) allenfalls nur die betroffenen Cluster bzw. die jeweiligen Ämter und Abteilungen ihre ausgewerteten Daten (nicht die Daten der anderen Cluster) erhalten.

- Die Rohdaten werden nach der Speicherung (empfohlen werden drei Monate; alternativ: 90 Tage) und nach dem Ende der Verkehrsmessung unwiederbringlich gelöscht. Das zu beauftragende Unternehmen wird darauf verpflichtet, die Löschung so durchzuführen, dass eine Wiederherstellung der Daten nicht möglich ist (s. u.: Weitergabekontrolle).

- Eine Weitergabe von Rohdaten an unberechtigte Dritte ist verboten. Auch der Auftraggeber (Universitätsstadt Gießen) erhält keine Rohdaten, um erneute ggf. kleinere Auswertungsraster zu verhindern.

- Intern ist ebenfalls festzulegen, wer die Auswertung (ohne die Rohdaten) erhält, da diese für die anstehenden Gespräche mit Betroffenen und zur Erstellung der Konzepte notwendig sind. Für die festgelegten Personen bzw. Gruppen (z. B. die Projektmitglieder einschließlich der Arbeitsgruppe) gelten das Weitergabeverbot und die weiteren Verpflichtungen sinngemäß. Die genannten Auswertungen werden innerhalb der Universitätsstadt Gießen daher nur im Sinne des Projektes weitergegeben, d.h. jedes Amt und jede Abteilung erhalten (nach vorheriger Festlegung der internen Kommunikationswege) allenfalls die eigenen Daten, nicht aber Auswertungen anderer Bereiche.

- Die Auftragskontrolle erfolgt über eine Verpflichtungserklärung, die der Stellungnahme als Anlage beigefügt wurde und die von dem zu beauftragenden Unternehmen unterzeichnet werden sollte."

Diese Stellungnahme bezog sich auf die Bewertung der vorgesehenen Maßnahme aus Sicht des behördlichen Datenschutzbeauftragten. Sie wurde als eine Vorleistung zu der nach § 6 HDSG zu erstellenden Verfahrensbeschreibung der Behörde bezeichnet. Es wurde weiterhin empfohlen, dass die Mitarbeiter/innen und der Personalrat/Gesamtpersonalrat vorab über die Maßnahme informiert werden.

Die Stellungnahme des Datenschutzbeauftragten ist den jeweiligen Projektverantwortlichen und Organisationseinheiten zugeleitet worden. Eine Auswertung der Umsetzung wird durch den behördlichen Datenschutzbeauftragten noch vorgenommen.

3. Schlussbemerkung

Um die Aufgaben sachgerecht erfüllen zu können, ist der behördliche Datenschutzbeauftragte in einem erforderlichen Umfang von der Erfüllung anderer Aufgaben freizustellen und mit entsprechenden Ressourcen auszustatten, damit eine ordnungsgemäße Wahrnehmung dieser Funktion sichergestellt ist. Hierzu zählen auch die zeitlichen Ressourcen, die wesentlich die Zeitnähe der Umsetzung der Aufgaben bestimmen.

Nach herrschender Auffassung wird für eine Kommune der Größenklasse der Universitätsstadt Gießen aufgrund der Anzahl der Beschäftigten und der Anzahl der IT-Arbeitsplätze die Umsetzung der Aufgabe in Form einer Vollzeitstelle empfohlen.

Für die Wahrnehmung der Aufgabe als Datenschutzbeauftragter und die Evaluation der Umsetzung der veranlassten Maßnahmen stehen dem Unterzeichner 25 % der täglichen Arbeitszeit zur Verfügung. Daneben erfordert die Aufgabe als Leiter des Revisionsamtes einen nahezu vollständigen Einsatz der verfügbaren, auch zeitlichen Ressourcen.

Insofern ist es nachvollziehbar, dass eine Selektion und Konzentration auf wesentliche Sachverhalte erfolgt. Dies gilt auch für die nun vorliegende, zusammenfassende Berichterstattung an die Gremien, die im genannten Zeitraum im Übrigen über die regelmäßige Informationen sowohl innerhalb der Behörde, als auch zeitnahe Aussagen zu datenschutzrechtlichen Sachverhalten sichergestellt war.

Entsprechend werden in eigener Zuständigkeit Prioritäten gesetzt und bestimmte Aufgaben auch zeitraumbezogen verschoben. In den Berichtsjahren konnten demzufolge gemeinsam mit den einzelnen Fachämtern - insbesondere dem Amt für Informationstechnik und dem Haupt- und Personalamt - im datenschutzrechtlichen Bereich sehr viele und notwendige, aber dennoch nicht alle Arbeitsaufträge, auch zum Schutze der Mitarbeiter/innen der Verwaltung, formuliert und umgesetzt werden.

Nach dem Hessischen Datenschutzgesetz noch umzusetzende Maßnahmen, wie z. B. die abschließende, datenschutzrechtliche Bewertung zur Dienstanweisung über den Einsatz von Zutrittskontrollsystemen und Videoüberwachungsanlagen, aber auch die Prüfung verschiedener, erforderlicher Verfahrensverzeichnisse und Vorabkontrollen nach §§ 6 ff. HDSG, sind z. T. in Zusammenarbeit mit den einzelnen Fachämtern noch abzuarbeiten.

Insbesondere zu letztem Sachverhalt ist es erforderlich, dass unter Hinweis auf die vorgesehene Vorabkontrollen alle Informationen und datenschutzrechtlichen Fragestellungen den behördlichen Datenschutzbeauftragten rechtzeitig erreichen. Dabei ist es von besonderer Bedeutung, dass der behördliche Datenschutzbeauftragte - ebenso wie das Revisionsamt - über den geplanten Einsatz entsprechender Softwareprodukte durch die Fachämter vorab informiert wird.

Ich bedanke mich bei allen Fachämtern und den KollegenInnen für die sehr positive Zusammenarbeit im Berichtszeitraum.

Gießen, 1.4.2012

H. Martin Lein
Behördlicher Datenschutzbeauftragter