Stadtverwaltung Cottbus
Büro des Oberbürgermeisters

Cottbus, 21.05.2010

Antwort zur Anfrage der Fraktion CDU, FDP, Frauenliste Cottbus zur Stadtverordnetenversammlung am 26. Mai 2010

„Stand Datenschutz und IT-Sicherheit in der Stadtverwaltung Cottbus"

Einleitung

In der modernen Informationsgesellschaft werden Computer und Computernetze immer wichtiger für die Geschäftsprozesse und die Erfüllung der Fachaufgaben. Behörden und Unternehmen sind inzwischen abhängig von der Informationstechnik, die große Datenmengen und vielfältige Informationen übermittelt, elektronisch verarbeitet und speichert. Die Institutionen sind zu ordnungsgemäßem und sicherem IT-Einsatz für den Umgang mit Verwaltungsdaten verpflichtet. Auch die Stadtverwaltung Cottbus sieht sich in der Pflicht, neben den im Brandenburgischen Datenschutzgesetz regulierten Maßnahmen zum sicheren Umgang mit personenbezogenen und sonstigen schützenswerten Daten, auch die technisch-organisatorischen Maßnahmen zum Schutz aller Informationen der Stadtverwaltung zu schaffen (Informationssicherheit). Diese Verpflichtung resultiert zum einen aus verschiedenen Landesgesetzen und Kabinettsbeschlüssen der Landesregierung, welche im Rahmen von Landesauftragsgeschäften durch die Stadt Cottbus verbindlich umzusetzen sind (beispielhaft sei hier die Übertragung des Status als Bewilligungsbehörde für Agrarfördermittel durch das Ministerium für Infrastruktur und Landwirtschaft des Landes Brandenburg benannt) sowie aus der moralischen Verantwortung gegenüber den Bürgerinnen und Bürgern der Stadt Cottbus, welche sich neben der vertraulichen Behandlung sämtlicher Informationen über den Datenschutz hinaus auch auf die Integrität, Verfügbarkeit, Authentizität und Transparenz im Umgang mit diesen Informationen verlassen können sollen.

Zu 1.) Mit welchem Arbeitsumfang arbeitet der behördliche Datenschutzbeauftragte (Beh. DSB) in der Stadtverwaltung Cottbus?

Die berufene behördliche Datenschutzbeauftragte, Frau Sabine Hiekel, ist laut Stellenbeschreibung mit einem Umfang von 0,25 VzE für die Erfüllung dieser Aufgaben tätig.

Zu 2.) Ist beabsichtigt, dass der Beh. DSB analog anderer Beauftragter in der Stadtverwaltung in größeren Abständen vor der Stadtverordnetenversammlung berichtet?

Entsprechend der Vorlage zur Entscheidung durch die Rathausspitze „Berichterstattung durch die Beauftragten in der Stadtverordnetenversammlung", beraten am 23.09.2009 in der Sitzung des Hauptausschusses, ist vorgesehen, die Berichterstattung der Beh. DSB auf Grund der sensiblen und schutzwürdigen Thematik lediglich im nichtöffentlichen Teil des Hauptausschusses durchzuführen. Da die Themenstel-

lung „Informationssicherheit“ zum Zeitpunkt der Beratung noch nicht aufgegriffen war, wurden diesbezüglich keine Vorschläge zur Berichterstattung unterbreitet. Auf Grund der nahe liegenden Aufgabenfelder wäre jedoch eine gemeinsame Berichtersterstattung plausibel.

Zu 3.) Existiert ein IT-Sicherheitsmanagement bzw. ein IT-Sicherheitskonzept in der Verwaltung und wenn ja, welche Maßnahmenschwerpunkte zur Abwendung von Gefahren und Risiken sind darin verankert?

Zu 4.) Gibt es einen IT-Sicherheitsbeauftragten in der Stadtverwaltung Cottbus?

Seit September 2009 gibt es in der Stadtverwaltung das Bestreben, die bereits bestehenden Maßnahmen zur Umsetzung einer sicheren IT-Infrastruktur und Informationsverarbeitung durch ein Informationssicherheitsmanagement zu steuern und in einem Sicherheitskonzept als strategische Grundlage zu definieren. Hierzu wurde ein IT-Sicherheitsbeauftragter, Herr Theodor Kubusch, vorerst benannt, der nach den entsprechenden personell-organisatorischen Maßnahmen die vollumfänglichen Aufgaben mit 0,6 VzE wahrnimmt. Die Stellenbeschreibung und Stellenbewertung erfolgt gegenwärtig.

Hierzu ist angestrebt, vorerst ein analytisches Grobkonzept zu erarbeiten, welches die zu betrachtenden IT-Verbünde sowie die Schutzbedarfskategorien festlegt und die Vorgehensweise zu Erfassung sämtlicher Anwendungen, Systeme und peripheren Einflussfaktoren beschreibt. Parallel werden hierzu die Maßnahmen zur Schaffung eines Informationssicherheitsmanagements eingeleitet und die operativen Aufgaben zur Umsetzung der technisch-organisatorischen Maßnahmen zur Informationssicherung (Teilschutzkonzepte, Risikoanalysen, Verfahrensverzeichnisse) wahrgenommen.

Die tatsächliche Schutzbedarfsfeststellung und ggf. notwendigen Risikoanalysen, deren Ergebnis das IT-Sicherheitskonzept darstellen, können erst nach den voran genannten Schritten umgesetzt werden.

Zu 5.) Wie ist ein notwendiger Datenaustausch zwischen der ARGE/Jobcenter, der Sozialverwaltung und der Jugendverwaltung geregelt?

Da Leistungsrechte von Betroffenen teilweise ineinander greifen (gemeinsame Schnittstellen), ist zwischen den Leistungsträgern zur Sicherung des Lebensunterhaltes nach SGB II (Jobcenter) und SGB XII (FB 50) und dem Träger der Jugendhilfe (FB 51) ein Datenaustausch zur optimalen Versorgung mitunter unabdingbar.

Dabei sind die Bestimmungen des Sozialdatenschutzes [Sozialgesetzbuch (SGB) I, § 35 sowie SGB X, §§ 67-85] und des Brandenburgischen Datenschutzgesetzes (Bbg DSG) zu wahren. Die Sozialleistungsträger (hier: FB 50, 51 und Jobcenter) sind nach § 86 SGB X verpflichtet, bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten. Für diese Zusammenarbeit bietet das SGB X in den §§ 68 bis 77 Übermittlungsbefugnisse. Solche Übermittlungsbefugnisse gibt es z. B.

- zur Bekämpfung von Leistungsmissbrauch und illegaler Ausländerbeschäftigung (vgl. § 67 e SGB X);

- für Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr oder zur Durchsetzung öffentlich-rechtlicher Ansprüche (vgl. § 68 SGB X)
- die Erfüllung sozialer Aufgaben (vgl. § 69 SGB X)
- für die Durchführung des Arbeitsschutzes (vgl. § 70 SGB X)
- für die Durchführung eines Strafverfahrens (vgl. § 73 SGB X)
- bei Verletzung der Unterhaltspflicht und beim Versorgungsausgleich (vgl. § 74 SGB X), um nur einige zu nennen.

Daneben ist die Übermittlung personenbezogener Daten von Betroffenen innerhalb der Stadtverwaltung gemäß § 14 Abs. 1 Bbg DSG zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder der Empfängerstelle erforderlich **oder** wenn eine Zweckänderung nach den Vorschriften des § 13 Abs. 2 Bbg DSG zulässig ist. Um eine Zweckänderung handelt es sich z. B.,

- wenn es erforderlich ist, die Angaben der betroffenen Person zu überprüfen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen (z. B. bei Leistungsmissbrauch),
- es zur Abwehr erheblicher Nachteile für das Gemeinwohl geht (z. B. der Erhalt der natürlichen Lebensgrundlagen und des Umweltschutzes) oder
- eine sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit besteht oder
- zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person (z. B. bei Kindeswohlgefährdung) erforderlich ist.

Durch die Behördliche Datenschutzbeauftragte wird in fachbereichsübergreifenden Beratungen, regelmäßig durchgeführten Datenschutzschulungen der Führungskräfte und Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung, in Einzelberatungen oder bei Datenschutzkontrollen immer wieder darauf verwiesen, dass Daten, die zwischen Mitgliedern einer Arbeitsgruppe austauscht werden, pseudonymisiert zu verwenden sind. D. h., dass der Name und andere Identifikationsmerkmale wie Geburtsdatum oder Anschrift der betroffenen Person durch ein Kennzeichen ersetzt werden, um die Bestimmung der Person auszuschließen oder wesentlich zu erschweren. (Mittels einer Referenzliste können die Kennzeichen / Pseudonyme den Betroffenen zugeordnet werden.) Denn in der Pseudonymisierung von Daten liegt ein praktikabler Lösungsansatz, um die Zusammenarbeit verschiedener Fachbereiche zu ermöglichen, ohne Klardaten hierbei zu verwenden, so z. B. für eine datenschutzrechtlich unproblematische Supervision oder die Erörterung von Fallkonstellationen in Teambesprechungen, Arbeitskreisen oder Fallkonferenzen. Im Fall des FB 51 fordert der Gesetzgeber sogar, dass vor einer Übermittlung an eine Fachkraft, die der verantwortlichen Stelle nicht angehört, Sozialdaten zu anonymisieren oder zu pseudonymisieren sind, soweit die Aufgabenerfüllung dies zulässt (vgl. § 64 Abs. 2a SGBVIII). In der täglichen Praxis der Leistungsträger wird von der Pseudonymisierung der Daten Gebrauch gemacht.

i. V. Jamitzky

Wieland Eschenburg
Bürgeiter des Oberbürgermeisters