16. Kommunales IuK-Forum Niedersachsen am 04./05.08.2016 in Goslar

Datenschutz – Aktuelle Herausforderungen

Vortrag am 04.08.2016 von Barbara Thiel, Landesbeauftragte für den Datenschutz

Zunächst darf ich mich herzlich für die Einladung hier nach Goslar bedanken! Schon aufgrund meiner bisherigen beruflichen Aktivitäten ist es mir eine besondere Freude, wieder einmal in der „kommunalen Familie“ zu Gast zu sein.

Die Aufgabe der Landesdatenschutzbeauftragten habe ich vor nunmehr 19 Monaten übernommen. Nie und nimmer hätte ich mir damals die große Bandbreite der Aufgaben vorstellen können, mit denen meine Behörde beschäftigt ist. Hinzu kommt, dass wir in Zeiten von Digitalisierung und Big Data gerade auch im technisch-organisatorischen Bereich in besonderem Maße gefordert sind. Lassen Sie mich deshalb kurz einen Blick auf die Behörde der Datenschutzbeauftragten des Landes Niedersachsen richten. Welche Stellung und welche Aufgaben hat die Landesbeauftragte für den Datenschutz in Niedersachsen überhaupt?

Die Behörde der Landesdatenschutzbeauftragten ist seit 2011 eine unabhängige oberste Landesbehörde und als solche ausdrücklich Verfassungsorgan. So heißt es in Art. 62 der Niedersächsischen Verfassung, dass die Landesbeauftragte für den Datenschutz „*unabhängig und nur an Gesetz und Recht gebunden*“ ist.

In der Verfassung sind gleichzeitig auch die Aufgaben der Datenschutzbeauftragten näher umschrieben: Sie hat, so bestimmt Art. 62, zu kontrollieren, „*dass die öffentliche Verwaltung bei dem Umgang mit personenbezogenen Daten Gesetz und Recht einhält*“. Das ist die klassische Kontrollfunktion der Datenschutzbehörde für ca. 5.500 Stellen in der öffentlichen Verwaltung in Niedersachsen und damit auch für die niedersächsischen Kommunen.

Daneben kommt der Landesdatenschutzbeauftragten nach dem niedersächsischen Datenschutzgesetz allerdings auch die Funktion einer Aufsichtsbehörde für den so

genannten nichtöffentlichen Bereich zu (§ 22 Abs. 6 NDSG). Hier in Niedersachsen sind wir damit für etwa 300.000 Wirtschaftsunternehmen zuständig. Hier, also bei der Wirtschaft, liegt nach meiner Einschätzung heute das Übergewicht bei der Verarbeitung personenbezogener Daten.

Meine Rolle im Datenschutz verstehe ich einerseits als die einer Wächterin bzw. Kontrolleurin. Zugleich sehe ich mich aber auch als „Dienstleisterin“ für die öffentliche Verwaltung und für die Wirtschaft. So heißt es im Landesdatenschutzgesetz ausdrücklich, dass die Datenschutzbeauftragte „*den Landtag, die Landesregierung, die übrigen Behörden und sonstigen öffentlichen Stellen über Verbesserungen des Datenschutzes beraten*“ kann (§ 22 Abs. 1 Satz 3 NDSG). Und nach § 38 Abs. 1 des Bundesdatenschutzgesetzes (BDSG), der Rechtsgrundlage für den nichtöffentlichen Bereich, „berät und unterstützt die Aufsichtsbehörde die Beauftragten für den Datenschutz in den Unternehmen und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse.“

Diesen Beratungsauftrag nehme ich sehr ernst. Zusammen mit meinen Mitarbeiterinnen und Mitarbeitern verstehe ich mich als kompetenten Ansprechpartner für Datenschutz und Datensicherheit. Dabei ist mir vorrangig daran gelegen, durch frühzeitige Beratung Datenschutzverstöße zu vermeiden.
Ich bin offen für zukunftsgerichtete Lösungen und bereit, gemeinsam mit den Beteiligten aus der Verwaltung und damit auch aus den Kommunen datenschutzgerechte Anwendungen zu entwickeln. Wir versuchen zu überzeugen und einvernehmliche Lösungen zu finden, sind im Konfliktfall aber auch bereit, datenschutzgerechtes Handeln gegen Widerstände durchzusetzen, denn das ist unser gesetzlicher Auftrag.

Gerade in den kommenden Monaten wird unser Beratungsauftrag eine ganz besondere Bedeutung haben. Denn das gesamte Datenschutzrecht steht vor grundlegenden Neuerungen. Damit komme ich auf die EU-Datenschutzreform zu sprechen.

Im Dezember letzten Jahres haben sich die Europäische Kommission, das Europäische Parlament und der Rat der Europäischen Union auf die lang erwartete Datenschutzreform verständigt. Diese Datenschutzreform besteht aus:

- der Datenschutzgrundverordnung, welche allgemein Datenschutzregeln für Private und für Behörden festlegt, und
- der Richtlinie für Datenschutz bei Polizei und Justiz, welche Datenschutz bei Strafverfolgung und Strafvollstreckung sicherstellt.

Die Datenschutzgrundverordnung ist am 25. Mai 2016 in Kraft getreten und wird nach einer Übergangszeit von 2 Jahren, also am 25.05.2018, in allen Staaten der Europäischen Union unmittelbar geltendes Recht. Die Inhalte der Richtlinie müssen demgegenüber vom Gesetzgeber zunächst in nationales Recht umgesetzt werden.

Das neue Datenschutzrecht bringt Veränderungen und damit zum Teil auch Unsicherheiten mit sich. Dennoch, und dieses Ergebnis möchte ich an den Anfang meiner Betrachtung stellen, bin ich der Meinung, dass diese Reform des Datenschutzrechts ihren Namen verdient und letztlich als Erfolg zu bewerten ist. Unter den modernen Bedingungen der Datenverarbeitung setzt die freie Entfaltung der Persönlichkeit den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Im digitalen Zeitalter brauchen wir hohe und zugleich einheitliche Datenschutzstandards, und hier wurden mit der Datenschutzgrundverordnung wesentliche Fortschritte erzielt.

In der EU gibt es zukünftig und anders als zuvor endlich eine weitgehende Einheitlichkeit für den Schutz personenbezogener Daten. Denn die Grundverordnung kommt in allen EU-Staaten direkt zur Anwendung. Das BDSG wird also zukünftig nur noch die Bereiche regeln können, in denen der EU-Gesetzgeber den Mitgliedsstaaten einen Regelungsspielraum gibt. Gegenwärtig ist noch offen, ob und inwieweit der Bundesgesetzgeber diese so genannten Öffnungsklauseln tatsächlich mit Leben füllen wird. Wir erwarten, dass wir bereits Mitte August einen ersten Entwurf dieses neuen Bundesdatenschutzgesetzes vorliegen haben werden.

Worin bestehen nun die großen Veränderungen, die durch diese Datenschutzreform bewirkt werden? Ganz allgemein lässt sich dazu sagen:

1. Das neue EU-Datenschutzrecht wird die Persönlichkeitsrechte der Bürgerinnen und Bürger stärken.
2. Der Wirtschaft wird ein einheitlicher, praxistauglicher Rahmen vorgegeben und damit werden europaweit fairere Wettbewerbsbedingungen geschaffen.
3. Schließlich und endlich erweitert die Grundverordnung die gesetzlichen Aufgaben und Zuständigkeiten der Aufsichtsbehörden. Das unterstützt den Datenschutz auch im Vollzug.

Mit der Datenschutzgrundverordnung werden gestärkte und auch neue individuelle Rechte des Einzelnen gegenüber den für die Verarbeitung von personenbezogenen Daten verantwortlichen Stellen begründet. Hierzu gehören die schon heute bekannten Rechte auf Auskunft, Korrektur und Löschung sowie die Informations- und Transparenzpflichten. Der Betroffene einer Datenverarbeitung kann in Zukunft vor allem erwarten, umfassender und verständlicher informiert zu werden. Die Ausübung der Betroffenenrechte muss für den Einzelnen zudem kostenfrei und ohne Hindernisse möglich sein. Die Grundverordnung gibt nun außerdem ausdrücklich vor, dass die Aufsichtsbehörde den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung aufgrund der Beschwerde unterrichten muss.

Gleichzeitig sehe ich auch gewisse Erleichterungen bei der Einreichung von Beschwerden durch Betroffene. So soll die Bereitstellung eines einheitlichen Beschwerdeformulars, das auch online zur Verfügung stehen soll (EG 141), die Hemmschwelle senken, mit Beschwerden an die Datenschutzbehörde heranzutreten. Es ist also damit zu rechnen, dass die Zahl der Eingaben, die in den letzten Jahren ohnehin schon deutlich gestiegen ist, in Zukunft noch größer werden wird.

Neu hinzugekommen sind mit der Datenschutzgrundverordnung das „Recht auf Vergessenwerden“ und das Recht der Nutzer, ihre Daten von einem kommerziellen Dienstleister wie etwa Facebook zu einem anderen mitzunehmen.

Gerade aus organisatorischer Sicht bedeutsam und neu sind auch der so genannte „One-Stop-Shop“ und das sog. Kohärenzverfahren. Jede betroffene Person kann sich künftig in ihrer eigenen Sprache an ihre eigene Aufsichtsbehörde in ihrem eigenen Land wenden und findet dort Gehör. Diese Aufsichtsbehörde bleibt Ansprechpartner im gesamten weiteren Verfahren. Dies ist für die Betroffenen eine große Erleichterung.

Vor allem aber ist der One-Stop-Shop für die Unternehmen eine bedeutsame Entlastung: Künftig haben sie es in Europa nur noch mit einer einzigen federführenden Aufsichtsbehörde zu tun, und zwar auch dann, wenn sie grenzüberschreitend tätig sind. Der Umgang mit unterschiedlichen Auffassungen in verschiedenen Ländern entfällt.

Als eine große Herausforderung für die Aufsichtsbehörden und ihre Arbeitsweise betrachte ich das Kohärenzverfahren. Bei Datenverarbeitungen, die nicht nur einen Mitgliedstaat betreffen, wird in Zukunft eine enge Zusammenarbeit aller betroffenen Aufsichtsbehörden erforderlich sein. Daraus resultiert ein Abstimmungsverfahren unter den Behörden, das ohne Zweifel ein sehr komplexes Gebilde sein wird.

Durchgesetzt hat sich in diesem Zusammenhang, dass die Aufsichtsbehörden sich im Streitfall auch per Mehrheitsentscheid zu einer gemeinsamen Linie verbindlich verpflichten können. Bei streitigen Fragen entscheidet letztlich der neu eingesetzte Europäische Datenschutzausschuss verbindlich und endgültig. Dieser wird die unverbindliche Arbeit der Art. 29-Arbeitsgruppe ablösen. Die Zuständigkeit für Datenverarbeitungen endet damit künftig nicht mehr an der Staatsgrenze.

Vor dem Hintergrund wesentlicher Grundprinzipien des Datenschutzes ist letztlich von besonderer Bedeutung, was mit der Grundverordnung gerade nicht geändert wurde: Der europäische Gesetzgeber hat sich dafür entschieden, den Grundsatz des Verbots mit Erlaubnisvorbehalt beizubehalten. Das heißt, jede Datenverarbeitung muss auf einer genau definierten Rechtsgrundlage beruhen und an einen genau bestimmten Zweck gebunden sein. Dieses Prinzip stand in den Verhandlungen zur Reform durchaus in der Kritik und damit auch zur Disposition.

Auch die Einwilligung bleibt ein entscheidender Grundpfeiler des Datenschutzes. Gleichzeitig stellt die Datenschutzgrundverordnung anders als die Richtlinie von 1995 unmissverständlich klar, dass jede Einwilligung nur durch eine eindeutig positiv bejahende Handlung konstituiert werden kann. Darüber hinaus muss die Einwilligung auch weiterhin informiert und frei gegeben werden.

Datenschutz ist ohne diese grundlegenden Prinzipien kaum durchsetzbar. Dies gilt ebenso für den ebenfalls in der Datenschutzgrundverordnung verankerten Grundsatz der Datensparsamkeit. Daher sind wir Aufsichtsbehörden sehr erleichtert, dass sich die tragenden Prinzipien des Grundrechtsschutzes hier letztlich doch durchgesetzt haben.

Für Sie als Vertreter der Kommunen dürfte in diesem Zusammenhang von besonderem Interesse sein, dass die Grundverordnung wichtige Neuerungen für die Datenschutzaufsicht im öffentlichen Bereich vorsieht.
Vorab ein paar Worte zum bisherigen Verfahren:

Stellt die LfD im Rahmen einer Prüfung datenschutzrechtliche Verstöße fest, so finden zunächst Gespräche mit der verantwortlichen Stelle statt, um einvernehmlich die festgestellten Mängel beim Datenschutz zu beseitigen.
Führen Gespräche mit der verantwortlichen Stelle nicht zum Erfolg, lehnt also die verantwortliche Behörde die Schaffung eines datenschutzkonformen Zustands ab, so kann die LfD von dem Mittel der förmlichen Beanstandung Gebrauch machen (§ 23 NDSG). Die Beanstandung wird mit der Aufforderung verbunden, innerhalb einer bestimmten Frist zu den festgestellten Mängeln Stellung zu nehmen und dabei auch die ergriffenen Abhilfemaßnahmen anzugeben.

Beanstandungen sind allerdings keine Verwaltungsakte. Sie können daher nicht vor dem Verwaltungsgericht angefochten werden. Damit besitzt die LfD auch keine Vollstreckungsmöglichkeiten. Bei einer Weigerung der öffentlichen Stelle, die datenschutzrechtlichen Mängel abzustellen, stehen der LfD folglich nach geltendem Recht keine Zwangsmaßnahmen oder Sanktionsmöglichkeiten zur Verfügung. Die LfD ist damit insoweit ein „Ritter ohne Schwert“.

Das wird sich mit der Datenschutzgrundverordnung ändern. So bestimmt Art. 58, dass wir Aufsichtsbehörden zukünftig auch gegenüber Behörden Anordnungen erlassen können, um beispielsweise rechtswidrige Datenverarbeitungen zu unterbinden, die Löschung personenbezogener Daten zu erwirken oder eine Übermittlung von Daten in Drittstaaten zu untersagen. Das bedeutet, dass die Aufsichtsbehörden zukünftig als spezifische Rechtsaufsichtsbehörden tätig werden können. Diesen Schritt hin zu einem Gleichklang zwischen den Befugnissen im öffentlichen und im nichtöffentlichen Bereich begrüße ich sehr.

In den kommenden Monaten wird es nun darum gehen, die neuen Regelungen einer genauen Analyse zu unterziehen, und zwar sowohl auf der Ebene des Bundes als auch in den Ländern. An dem Prozess, der jetzt vor uns liegt, werden wir konstruktiv teilnehmen und Ihnen bei Bedarf auch gern beratend zur Seite stehen. Machen Sie von unserem Beratungsangebot Gebrauch!

Nun komme ich zu einem ganz aktuellen Gesetzgebungsvorhaben, das auch meine Behörde intensiv beschäftigt hat:

Am Dienstag dieser Woche hat die Landesregierung Gesetz zur Änderung des niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung auf den Weg gebracht. Schon aus

alter Verbundenheit zu den Kommunen habe ich sehr genau verfolgt, dass die kommunalen Spitzenverbände vehement dafür eingetreten sind, den Begriff der öffentlichen Ordnung nicht zu streichen. Leider erfolglos!

Der Gesetzentwurf enthält eine Vielzahl von Regelungen, die den Datenschutz betreffen. Ich hatte daher die Gelegenheit, im Rahmen der Verbandsbeteiligung ausführlich zum Gesetzentwurf Stellung zu nehmen. Verständlicherweise wurden nicht alle meine Forderungen aufgegriffen. Jedoch möchte ich auf eine Norm aufmerksam machen, die zukünftig für die Kommunen von Bedeutung sein kann: die Neuregelung der so genannten Abschnitts-Geschwindigkeitskontrolle, auch Section Control genannt.

Die Pilotanlage, die auf Betreiben des Innenministers auf der B 6 bei Hannover aufgebaut wurde, stand bisher rechtlich gesehen auf mehr als wackeligen Füssen. Klar ist, dass für einen regulären Betrieb eine gesetzliche Grundlage zwingend erforderlich ist. Denn mit dem Autokennzeichen erhebt die Anlage ein personenbezogenes Datum.

Insofern freut es mich besonders, dass meine Forderung nach einer gesetzlichen Grundlage in dem Gesetzentwurf nunmehr umgesetzt wurde. Der Gesetzentwurf ist so formuliert, dass nicht nur die Polizei sondern auch die Verwaltungsbehörden eine derartige Anlage betreiben können. Dies setzt allerdings voraus, dass das Pilotprojekt des Innenministeriums erfolgreich abgeschlossen wird.

In den vergangenen Jahren hat mein Vorgänger Joachim Wahlbrink einen Schwerpunkt seiner Arbeit in der Videoüberwachung im nichtöffentlichen Bereich gesehen. Nach wie vor erreichen uns fast wöchentlich Eingaben besorgter Bürgerinnen und Bürger, die sich über die Installation von Videokameras im Eingangsbereich von Büro- oder Wohngebäuden oder vor und in Verkaufsräumen beschweren.

Gegenwärtig führe ich zudem einen Rechtsstreit mit dem Hannoverschen Nahverkehrsunternehmen Üstra AG, das in seinen Bussen und Bahnen fast flächendeckend Videoüberwachung einsetzt. Das Bildmaterial wird auf einem sog. Ringspeicher im Fahrzeug für 24 Stunden zwischengespeichert und anschließend überschrieben; im Bedarfsfall werden Videoaufzeichnungen anlassbezogen vor Überschreibung gesichert, eine sonstige Zugriffsmöglichkeit, insbesondere die Möglichkeit einer Echtzeitüberwachung, besteht nicht. Dieses Verfahren hat bundesweit einmaligen Pilotcharakter.

Um es gleich vorwegzunehmen: Ich bin keineswegs generell gegen Videoüberwachung. Nach meiner Auffassung widersprechen die Kameras in den Hannoverschen Bussen und Bahnen allerdings dem BDSG. Insbesondere hat das Verkehrsunternehmen bisher nicht darlegen können, dass die Videoüberwachung in ihrem konkret praktizierten Umfang tatsächlich zur Abwehr ganz konkreter Gefahren erforderlich ist.

Auch aus polizeilicher Sicht sind Gefahrenlagen und das Straftatengeschehen in den Fahrzeugen gering. Die Erforderlichkeit eines umfassenden Kameraeinsatzes ist deshalb nicht erkennbar.

Der Ausgang des Rechtsstreits ist noch offen. Gegenwärtig sind wir noch gar nicht zu den inhaltlichen Fragen vorgedrungen. Vor dem Verwaltungsgericht und damit in der ersten Instanz ging es bisher ausschließlich um die Frage, ob die Üstra als privates Unternehmen – so unsere Auffassung – oder als ein nicht am Wettbewerb teilnehmendes und von der öffentlichen Hand, nämlich der Region Hannover, beherrschtes Unternehmen anzusehen ist. Von der Beantwortung dieser Frage hängt ab, ob etwaige datenschutzrechtliche Verstöße des Nahverkehrsunternehmens untersagt und letztlich sanktioniert werden können.

Da das Verwaltungsgericht in seinem Urteil von der Anwendung des Landesdatenschutzgesetzes ausgeht, habe ich Berufung eingelegt. Ich hoffe darauf, dass wir uns vor dem Oberverwaltungsgericht endlich dem wichtigen Problem zuwenden werden, in welchem Umfang die Videoüberwachung in Fahrzeugen des öffentlichen Personennahverkehrs tatsächlich datenschutzkonform betrieben werden kann und ob dem immer wieder angeführten Abschreckungseffekt und dem subjektiven Sicherheitsgefühl der Bevölkerung künftig eine verstärkte Bedeutung beigemessen werden muss.

Lassen Sie mich jetzt auf einige konkrete aktuelle datenschutzrechtliche Fragestellungen zu sprechen kommen, die insbesondere für die Kommunen von Interesse sind.

Bei einer Vorort-Beratung in einer Kommune, die meine Mitarbeiterinnen und Mitarbeiter durchgeführt haben, ist jüngst eine Führerscheinstelle als besonderer Problemfall in den Fokus gerückt. In der Führerscheinstelle waren in einem Raum von ca. 30 qm mehrere Beratungsplätze nebeneinander untergebracht. Zeitgleich wurden mehrere Beratungsgespräche geführt. Gerade in einer Führerscheinstelle, in der hochvertrauliche Daten wie Gesundheitsdaten oder sogar Daten über Straftaten offenbart werden, ist allerdings äußerste Diskretion geboten.

Diesen Einzelfall, bei dem die besagten gravierenden Mängel festgestellt worden sind, habe ich zum Anlass genommen, alle Führerscheinstellen in Niedersachsen zu überprüfen. Derzeit wird zur Vorbereitung der Prüfung ein Fragebogen erstellt, der anschließend an alle Kommunen versandt wird, die das Fahrerlaubnisrecht bearbeiten. Schon jetzt bin ich gespannt auf die Ergebnisse.

Diese Prüfung ist ein guter Anlass, noch einmal grundsätzlich auf die datenschutzrechtlichen Probleme beim persönlichen Kontakt der Bürgerinnen und Bürger mit ihrer Kommune einzugehen. Die Annahme von Führerscheinanträgen erfolgt bekanntlich nicht selten in den so genannten Bürgerbüros. Fast alle Städte und Gemeinden bieten heutzutage Dienstleistungen in „Bürgerbüros“ bzw. in multifunktionalen Servicebereichen unter ähnlicher Bezeichnung („Bürgeramt, Bürgerladen, Servicecenter“) an.

Das zentrale Ziel ist dabei vor allem, den Kontakt von Bürgerinnen und Bürgern zur Verwaltung schneller, einfacher und effektiver zu gestalten. Bedurfte es früher mehrfacher Behördengänge für verschiedene Anliegen, so können heute viele Aufgaben an demselben Arbeitsplatz von ein und derselben Mitarbeiterin bzw. Mitarbeiter der Kommune erledigt werden. Die Mitarbeiterinnen und Mitarbeiter der Bürgerbüros erhalten auf diese Weise tagtäglich umfassende Informationen aus den verschiedensten Lebensbereichen einzelner Bürgerinnen und Bürger.

Die Konzentration auf eine Ansprechstelle bietet aus Sicht einer serviceorientierten Verwaltung einen echten Mehrwert für die Bürgerinnen und Bürger. Gegen Bürgerbüros ist aus datenschutzrechtlicher Sicht grundsätzlich nichts einzuwenden. Ihre Einrichtung setzt allerdings voraus, dass die datenschutzrechtlichen Vorgaben beachtet werden. Hierzu hat meine Behörde schon in der Vergangenheit eine im Internet abrufbare Checkliste entwickelt.

Die wichtigsten fünf Punkte möchte ich hier kurz skizzieren.

1. Von vornherein muss baulich sichergestellt sein, dass Unbefugte von personenbezogenen Daten der Bürgerinnen und Bürger keinerlei Kenntnis erlangen können. Die räumlichen Verhältnisse im Bürgerbüro müssen aus diesem Grund auch

eine Einzelberatung zulassen. Für vertrauliche Gespräche sollen neben dem Großraumbüro auch separate Einzelberatungsplätze zur Verfügung stehen. Durch ein gut sichtbares Hinweisschild sollten Bürgerinnen und Bürger auf die Möglichkeit der Einzelberatung hingewiesen werden.

2. Der Zugriff auf Daten des Fachamtes durch das Bürgerbüro muss von der Einwilligung der Antragstellerin bzw. des Antragstellers abhängig gemacht werden; eine Speicherung der Daten außerhalb des Fachamtes muss unterbleiben (Vermeidung doppelter Datenspeicherung).

3. Aufgabenbereiche, in denen besonders sensible Daten verarbeitet werden, wie z. B. Sozialleistungen oder Steuerangelegenheiten, sollten nicht im Bürgerbüro bearbeitet werden.

4. Aufgabenbereiche, in denen die Datenverarbeitung besonderen Geheimhaltungsvorschriften unterliegt, wie z. B. das Standesamtswesen oder die Personaldatenverarbeitung, dürfen nicht im Bürgerbüro abgewickelt werden.

5. Es bedarf klarer Dienstanweisungen zum Umgang mit personenbezogenen Daten. Bei umfassender Zuständigkeit eines Bürgerbüros für verschiedene Aufgaben sind die Zuständigkeiten unter den Mitarbeiterinnen und Mitarbeitern in einem Rollen- und Zugriffsberechtigungskonzept festzulegen.

Ein weiteres Thema, welches ich hier kurz anreißen möchte, sind die Ratsinformationssysteme. Dieses Thema klingt vielleicht unspektakulär. Aber gerade in den letzten Monaten hatten wir eine Vielzahl von Eingaben besorgter Bürgerinnen und Bürger und auch von Ratsmitgliedern, die ihre Persönlichkeitsrechte in den kommunalen Vertretungskörperschaften und Ausschüssen nicht ausreichend gewahrt sahen.

Automatisierte Rats- und Bürgerinformationssysteme werden bekanntlich mittlerweile in einer Vielzahl der niedersächsischen Städte, Gemeinden und Landkreise eingesetzt. Diese Informationssysteme erlauben es der Verwaltung, den kommunalen Sitzungsdienst effizient zu steuern. Gleichzeitig können sich die

ehrenamtlichen Mandatsträgerinnen und –träger sowie die Bürgerinnen und Bürger zeitnah über die in den kommunalen Gremien zur Beratung oder Beschlussfassung anstehenden Themen informieren. So werden vielfach nicht nur die Tagesordnung der kommunalen Gremien, sondern auch die zur Beratung und Beschlussfassung anstehenden Vorlagen sowie die Niederschriften der Sitzungen in das öffentlich zugängliche kommunale Internetangebot eingestellt.

Aber: In den kommunalen Vertretungskörperschaften und Ausschüssen werden auch schützenswerte und vertrauliche Angelegenheiten behandelt. Denken Sie nur an die Beschlussfassung zu Personalangelegenheiten, zu Auftragsvergaben, zur Vermietung oder Verpachtung kommunaler Einrichtungen, zu Vertragsangelegenheiten, zur Festsetzung kommunaler Abgaben und Gebühren oder über Anregungen und Beschwerden der Bürgerinnen und Bürger etwa im Rahmen der Bauleitplanung. Es liegt auf der Hand, dass in solchen Beratungsdokumenten regelmäßig schützenswerte personenbezogene Daten enthalten sind. Der Grundsatz der Öffentlichkeit von Sitzungen der Vertretungen nach § 64 NKomVG kann deshalb an dieser Stelle nicht gelten.

Und Vorgänge, die aufgrund berechtigter Interessen der Betroffenen in nichtöffentlicher Sitzung zu behandeln sind, dürfen ohne das vorherige Einverständnis der Betroffenen einer breiten Öffentlichkeit nicht zugänglich gemacht werden. Ihre Veröffentlichung im öffentlich zugänglichen Teil eines Ratsinformationssystems ist daher nicht zulässig. Im Übrigen kann, wenn eine Angelegenheit in öffentlicher Sitzung zu behandeln ist, ein Personenbezug oder eine Personenbeziehbarkeit durch Anonymisierung oder Pseudonymisierung vermieden werden.

Ich komme zu einem weiteren Thema, das gegenwärtig in den Kommunen diskutiert wird: Immer mehr Kommunen möchten öffentliche Sitzungen via Live-Stream über das Internet oder über örtliche Fernsehsender übertragen lassen.

Wie Sie wissen, fehlt es in Niedersachsen derzeit noch an einer entsprechenden Rechtsgrundlage. Daher gilt zurzeit für Live-Übertragungen das Einwilligungserfordernis. Und zwar für alle Betroffenen. Es dürfen also nur diejenigen

Abgeordneten zu sehen und zu hören sein, die vorab ihre schriftliche Einwilligung erteilt haben. Zudem ist zu gewährleisten, dass sämtliche Wortmeldungen und Zwischenrufe auch von Bürgerinnen und Bürger nicht übertragen werden.

Der Rechtsrahmen soll sich allerdings ändern. Denn in dem von der Landesregierung verabschiedeten und in den Landtag eingebrachten Gesetzentwurf zur Novellierung des NKomVG ist auch eine Regelung zu Bild- und Tonaufzeichnungen in Ratssitzungen vorgesehen.

So heißt es in § 64 Abs. 2 des Gesetzentwurfs: „*Die Vertretung kann durch Hauptsatzung bestimmen, dass in öffentlichen Sitzungen Film- und Tonaufnahmen von den Mitgliedern der Vertretung mit dem Ziel der Veröffentlichung zulässig sind. Abgeordnete der Vertretung können verlangen, dass die Übertragung oder Aufnahme ihres Redebeitrages unterbleibt.*“

Die gesetzliche Regelung will also nur den Abgeordneten ein ausdrückliches Widerspruchsrecht einräumen. Hinsichtlich der übrigen Anwesenden in einer öffentlichen Sitzung, deren Persönlichkeitsrechte bei einer Liveübertragung ebenso tangiert sein können, schweigt der Gesetzgeber. An den Ratssitzungen nehmen neben den Abgeordneten regelmäßig aber auch Bürgerinnen und Bürger oder Bedienstete teil. Für diesen Personenkreis soll nach der Gesetzesbegründung weiterhin das Einwilligungserfordernis zur Bild- und Tonaufzeichnung mit dem Ziel der Veröffentlichung gelten. Hinsichtlich der Verantwortlichkeit für die Einhaltung des Datenschutzes heißt es in der Begründung ferner: „*Soweit Übertragungen von Medien (Fernsehen, Rundfunk usw.) vorgenommen werden, haben diese die Persönlichkeitsrechte zu beachten. Erfolgt die Übertragung durch die Kommune selbst, sind sie für den Schutz der Persönlichkeitsrechte verantwortlich.*“

In meiner Stellungnahme zum Gesetzentwurf habe ich grundsätzlich begrüßt, dass zukünftig die Fälle der Live-Übertragungen ausdrücklich gesetzlich geregelt werden. Kritisch habe ich mich allerdings dazu geäußert, dass in dem vorgelegten Änderungsentwurf des § 64 NKomVG lediglich Regelungen für Abgeordnete, nicht aber für die übrigen Anwesenden in einer öffentlichen Sitzung getroffen werden sollen. Ich habe daher aus Gründen der Normenklarheit die Empfehlung

ausgesprochen, den neuen Absatz 2 dahingehend zu ergänzen, dass Bild- und Tonaufzeichnungen grundsätzlich nur von Abgeordneten zulässig sind. Dritte, also anwesende Bürgerinnen und Bürger oder Bedienstete, müssen ausdrücklich schriftlich einwilligen. Auch das Einwilligungserfordernis der übrigen Beteiligten muss gesetzlich verankert werden. Nur dann sind die Rahmenbedingungen für eine Live-Übertragung einer Ratssitzung mittels Live-Streaming im Internet oder Fernsehübertragung klar geregelt. Das gilt im Übrigen unabhängig davon, wer die Übertragung zu verantworten hat – die Kommunalverwaltung oder ein Fernsehsender.

Der Gesetzentwurf befindet sich derzeit in der Landtagsberatung. Es bleibt zu hoffen, dass in den nunmehr stattfindenden Ausschussberatungen die Regelung des § 64 Abs. 2 klarer und bestimmter im oben beschriebenen Sinne gefasst wird, so dass für alle Beteiligten Rechtssicherheit besteht.

In den letzten Jahren hat die Nutzung von mobilen Endgeräten wie Tablets auch in der Ratsarbeit Einzug gehalten. Immer wieder werden wir gefragt, wie dies datenschutzrechtlich zu bewerten ist. Auch hierzu ein paar Hinweise:

Für die Datenverarbeitung durch kommunale Mandatsträgerinnen und -trägern findet das NDSG Anwendung.
Mandatsträgerinnen und –träger dürfen demnach personenbezogene Daten nur verarbeiten, soweit dies zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich ist. Zudem sind sie gem. § 40 NKomVG zur Verschwiegenheit verpflichtet. Die Mandatsträgerinnen und -träger sind daher ebenso wie die Behörde selbst dazu verpflichtet, die datenschutzrechtlichen Vorschriften zu beachten und die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit zu treffen.

Wenn die Mandatsträgerinnen und –träger private Geräte nutzen wollen, sind sie bei der Einhaltung der skizzierten Normen regelmäßig überfordert. Deshalb begrüße ich es sehr, dass einige Kommunen in Niedersachsen dazu übergegangen sind, ihren Vertretungen mobile Endgeräte wie z. B. Tablets für die Gremienarbeit zur Verfügung

stellen. Aus datenschutzrechtlicher Sicht ist das die zu favorisierende Lösung. Die Nutzung privater Endgeräte kann dann in der Gremienarbeit unterbleiben.

Die bereitgestellte Hardware hat zudem den Vorteil, dass die bereits vorhandene IT-Infrastruktur der Kommune genutzt werden kann und die Geräteauswahl, die Nutzungsregelungen sowie insbesondere auch die entsprechenden Datensicherungsmaßnamen von der Verwaltung vorgegeben werden.

Erlauben Sie mir abschließend noch einen Hinweis:

In diesem Jahr finden in Niedersachsen Kommunalwahlen statt, sodass einige der derzeit tätigen Mandatsträgerinnen und –träger ausscheiden und andere wiederum neu in das Amt gewählt werden. Für die neu ins Amt gewählten Abgeordneten ist es außerordentlich wichtig, dass ihnen fachliche und rechtliche Unterstützung für ihre neue Tätigkeit gegeben wird.

Ich bin daher auch gerne der Bitte nachgekommen, einen Artikel für das Taschenbuch des NSGB für Ratsmitglieder zu schreiben. Für diese Möglichkeit bedanke ich mich an dieser Stelle noch einmal recht herzlich. In diesem Artikel habe ich die wichtigsten ersten Informationen zum Thema Datenschutz für neu gewählte Abgeordnete zusammengestellt. Sollten in der täglichen Arbeit darüber hinaus datenschutzrechtliche Fragen auftreten, können sich die Abgeordneten – und natürlich auch Sie – jederzeit an mich und mein Team wenden. Wir geben Ihnen gern Auskunft und stehen Ihnen beratend zur Seite.

Vielen Dank für Ihre Aufmerksamkeit!