

Orientierungshilfe zum Datenschutz für kommunale Abgeordnete

Herausgeberin:

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5, 30159 Hannover

Tel.: 0511 120-4500

Fax: 0511 120-4599

E-Mail: poststelle@lfd.niedersachsen.de

Stand: Oktober 2016

Inhaltsverzeichnis

Vorwort

1. Datenschutz, was geht mich das an?	S. 4
1.1 Das Recht auf informationelle Selbstbestimmung	S. 4
1.2 Wichtige Begriffe im Umgang mit personenbezogenen Daten	S. 5
2. Sechs elementare Schutzziele	S. 6
3. Ratsarbeit und Datenschutz	S. 7
4. Ratsinformationssysteme	S. 21
5. Wie sichern Sie als Abgeordnete Ihre technischen Geräte, die Sie für die Gremienarbeit nutzen?	S. 21
6. Weiterführende Links	S. 22
7. Die Landesbeauftragte für den Datenschutz Niedersachsen	S. 23

Vorwort

Sehr geehrte Leserin, sehr geehrter Leser,

am 11. September 2016 fanden in Niedersachsen die Kommunalwahlen statt. Zum Beginn der Wahlperiode am 1. November 2016 nehmen die gewählten Abgeordneten ihre Arbeit in den Kommunalparlamenten auf. Die Übernahme eines solchen Amtes ist geprägt von vielen neuen Eindrücken und Herausforderungen.

Eine der Herausforderungen in der Gremienarbeit ist es, den Balanceakt zwischen dem allgemeinen Informationsinteresse der Bürgerinnen und Bürger auf der einen Seite und dem Recht auf informationelle Selbstbestimmung jedes Einzelnen auf der anderen Seite zu meistern. Diese Orientierungshilfe habe ich speziell für kommunale Abgeordnete zusammengestellt. Sie soll dazu beitragen, das Bewusstsein für den Datenschutz zu schärfen und Sachverhalte unter datenschutzrechtlichen Gesichtspunkten bewerten zu können.

Meine Aufgabe als Landesbeauftragte für den Datenschutz Niedersachsen ist es, darauf zu achten, dass das Recht auf informationelle Selbstbestimmung jedes Einzelnen geschützt wird. Ich bin davon überzeugt, dass es den gewählten Abgeordneten ebenfalls gelingen wird, den Datenschutz in ihrer täglichen Arbeit nicht aus den Augen zu verlieren.

Allen Leserinnen und Lesern wünsche ich nunmehr eine anregende Lektüre und den Abgeordneten viel Erfolg bei der Wahrnehmung der neuen Aufgabe.

Barbara Thiel
Landesbeauftragte für den Datenschutz Niedersachsen

Hannover, im Oktober 2016

1. Datenschutz, was geht mich das an?

„Stadtrat tagt öffentlich“, „Kommunalwahl: Partei will Auskunft aus dem Melderegister“, „Bürgermeister gratuliert zur Goldenen Hochzeit“,

Diese oder ähnliche Schlagzeilen sind häufig in der Tageszeitung zu finden. Manchmal ist es auch das frühmorgendliche Gespräch mit Bürgerinnen und Bürgern in der Warteschlange beim Bäcker. Abgeordnete werden dort vielleicht gefragt, wer denn der nächste Kämmerer bzw. die nächste Kämmerin wird oder wer die vakante Stelle in einem Dezernat bekommen soll. Selbstverständlich wissen sie über diese Angelegenheiten Bescheid. Was aber müssen Abgeordnete in solchen Situationen datenschutzrechtlich beachten?

Diese Orientierungshilfe soll Abgeordneten helfen, datenschutzrelevante Sachverhalte im Rahmen ihrer ehrenamtlichen Tätigkeit zu erkennen und einzuordnen. Sie soll sie in die Lage versetzen, datenschutzrechtliche Problematiken zu bewerten und dabei unterstützen, ein Gespür für den Umgang mit personenbezogenen Daten zu entwickeln.

1.1. Das Recht auf informationelle Selbstbestimmung

Grundsatz:

Meine Daten gehören mir - das Recht auf informationelle Selbstbestimmung

Wenn von schützenswerten Daten die Rede ist, so handelt es sich hierbei nicht um anonyme Zahlen oder Statistiken, sondern es geht um die personenbezogenen Daten der Mitbürgerinnen und Mitbürger, oder aber der Abgeordneten selbst.

Das Bundesverfassungsgericht hat mit dem so genannten Volkszählungsurteil vom 15.12.1983 (BVerfGE 65,1 ff.) grundlegende Aussagen zum Umgang mit personenbezogenen Daten getroffen und aus dem Grundrecht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 Grundgesetz - GG) in Verbindung mit der Würde des Menschen (Art. 1 Abs. 1 GG) das Recht auf informationelle Selbstbestimmung abgeleitet. Der Richterspruch aus Karlsruhe verleiht dem Recht auf informationelle Selbstbestimmung den Charakter eines Grundrechts:

„Das Grundrecht auf informationelle Selbstbestimmung gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig.“

Ganz ähnlich lautet dann auch § 1 des Niedersächsischen Datenschutzgesetzes (NDSG):

„Aufgabe dieses Gesetzes ist es, das Recht einer jeden Person zu gewährleisten, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen (Recht auf informationelle Selbstbestimmung). Dieses Gesetz bestimmt, unter welchen

Voraussetzungen personenbezogene Daten durch öffentliche Stellen verarbeitet werden dürfen.“

1.2. Wichtige Begriffe im Umgang mit personenbezogenen Daten

Datenschutz bedeutet nicht abstrakt, dass irgendwelche Daten geschützt werden. Datenschutz bedeutet vielmehr, dass die Betroffenen vor einer unrechtmäßigen Verwendung ihrer Daten geschützt werden. Er ist Teil des verfassungsrechtlichen Selbstbestimmungsrechts und des Schutzes der Persönlichkeit.

Personenbezogene Angaben über die rassische oder ethnische Zugehörigkeit, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualeben sind **besonders sensible Daten** und daher als besonders schutzwürdig anzusehen.

Der Oberbegriff für den Umgang mit personenbezogenen Daten lautet **Datenverarbeitung**. Die Verarbeitung von Daten ist nur zulässig, soweit das NDSG oder eine andere Rechtsvorschrift dies vorsieht oder die Betroffenen eingewilligt haben. Eine Rechtsvorschrift i. S. d. NDSG ist unter anderem ein Gesetz, eine Rechtsverordnung oder eine Satzung.

Sollen Daten durch eine öffentliche Stelle verarbeitet werden, ist in jedem Fall der Grundsatz der **Erforderlichkeit** zu beachten. Er besagt, dass vor einer Datenverarbeitung für jedes einzelne Datum die Datenverarbeitung einer Prüfung auf Eignung, Notwendigkeit und Verhältnismäßigkeit zu unterziehen ist.

Das Prinzip der **Zweckbindung** verlangt, dass Daten grundsätzlich nur zu dem Zweck verarbeitet werden dürfen, für den sie erhoben worden sind.

Ein weiterer wichtiger Begriff im Datenschutzrecht ist die **Datenübermittlung**. Sie bedeutet das Bekanntgeben von Daten an Dritte in der Weise, dass die Daten durch die Daten verarbeitende Stelle weitergegeben werden oder Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsehen oder abrufen. Die Datenübermittlung ist grundsätzlich nur zulässig, soweit eine Rechtsvorschrift sie erlaubt oder eine Einwilligung der Betroffenen vorliegt und der Grundsatz der Erforderlichkeit beachtet wurde.

Datensicherung umfasst die Summe aller technischen und organisatorischen Sicherungsmaßnahmen, die erforderlich sind, um eine den Datenschutznormen entsprechende Datenverarbeitung sicherzustellen. Ziel ist ein angemessenes Maß an Datensicherheit.

Unter **Datenvermeidung und Datensparsamkeit** versteht man ein Grundprinzip für die Ausgestaltung und den Betrieb technischer Datenverarbeitungssysteme. Dabei soll sowohl bei Entwicklung und Auswahl als auch beim laufenden Betrieb technischer Datenverarbeitungssysteme darauf hingewirkt werden, keine oder möglichst wenig personenbezogene Daten zu verarbeiten.

Ergänzend zum Begriff der Datensparsamkeit gilt der Grundsatz der **Datenvermeidung**. Er fordert, dass bereits im Vorfeld zu prüfen und zu klären ist,

welche Daten für den jeweiligen Zweck tatsächlich benötigt werden. Dazu gehört die Feststellung, ob überhaupt personenbezogene Daten verwendet werden müssen, oder ob auf die Erhebung personenbezogener Daten ganz verzichtet werden kann. Der Grundsatz der Datenvermeidung ist dem Grundsatz der Datensparsamkeit übergeordnet.

Eine weitere wichtige Säule im Datenschutzrecht ist das sog. **Transparenzgebot**. Es bedeutet, dass grundsätzlich jede Bürgerin und jeder Bürger jederzeit wissen können muss, wer was von ihr oder ihm bei welcher Gelegenheit weiß. Aus diesem Grund ist jede Daten verarbeitende Stelle verpflichtet, den Betroffenen Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen. Dieses Recht darf nur unter ganz engen und nur in den gesetzlich geregelten Fällen versagt werden (§ 16 Abs. 4 NDSG)!

In seiner Entscheidung zur Online-Durchsuchung hat das Bundesverfassungsgericht am 27.02.2007 – BvR 370/07, 1 BvR 595/07 - festgestellt, dass das allgemeine Persönlichkeitsrecht auch das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** umfasst.

2. Sechs elementare Schutzziele

Neben den rechtlichen Vorgaben sind insbesondere beim Einsatz automatisierter Verfahren die technisch-organisatorischen Maßgaben und Schutzziele zu beachten (Ableitung aus § 7 NDSG). Eine den heutigen und auch künftigen Anforderungen einer komplexen IT-Welt gerecht werdende Definition des Schutzbereiches im Sinne des Datenschutzes sollte die sechs folgenden Kernziele umfassen:

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte auf Verfahren und Daten zugreifen und zur Kenntnis nehmen können (**Vertraulichkeit**),
2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (**Integrität**),
3. Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (**Verfügbarkeit**),
4. die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (**Transparenz**),
5. personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (**Nichtverkettbarkeit**) und
6. Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte (z. B. nach den §§ 16 ff) wirksam ermöglichen (**Intervenierbarkeit**).

Aus diesen elementaren Schutzziele lassen sich weitere – aus Rechtsprechung und Kommentierung teils wohlbekannte - Anforderungen ableiten, die je nach Anwendungsszenario zur Beurteilung zusätzlicher Teilaspekte einer datenschutzgerechten Verfahrensgestaltung herangezogen werden können.

So ist im Einzelfall zu fordern, dass bei der automatisierten Verarbeitung personenbezogener Daten auch Maßnahmen zu treffen sind, die gewährleisten, dass u. a. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (**Authentizität, Teil der Integrität**), festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (**Revisionsfähigkeit; Teil der Transparenz**).

Die Schutzziele dienen als umfassender Maßstab für die Zielbestimmung, die sich aus den Grundrechten und der Rechtsprechung des Bundesverfassungsgerichtes (Persönlichkeitsrechte, Recht auf informationelle Selbstbestimmung, Schutzanspruch auf Integrität und Vertraulichkeit informationstechnischer Systeme) ergibt. Sie sind insbesondere geeignet die Basis für eine systematisierte technisch-organisatorische Ausgestaltung oder Prüfung von informationstechnischen Systemen (Hard- und Software), von geplanten und implementierten IT-Verfahren sowie der damit einhergehenden Abläufe und Geschäftsprozesse zu bilden. In der Praxis bedeutet dies, dass sich auf dieser Grundlage der Schutzziele der erforderliche Katalog von konkreten Datenschutzmaßnahmen entwickeln lässt.

3. Ratsarbeit und Datenschutz

Die Grundsätze der ehrenamtlichen Tätigkeit als Abgeordnete sind im Niedersächsischen Kommunalverfassungsrecht (NKomVG) geregelt.

Eine sehr wesentliche und datenschutzrechtlich bedeutsame Regelung enthält § 40 NKomVG. Hiermit werden die Abgeordneten zur **Amtsverschwiegenheit** verpflichtet.

Das bedeutet, dass Abgeordnete niemandem Auskunft über Dinge erteilen dürfen, die sie im Rahmen ihrer ehrenamtlichen Tätigkeit erfahren haben und die der Geheimhaltung unterliegen. Die Amtverschwiegenheit betrifft insbesondere vertrauliche Angelegenheiten, die in nicht-öffentlicher Sitzung behandelt werden.

Grundsatz: Die Sitzungen der Vertretung sind öffentlich.

Die Sitzungen der Vertretung sind öffentlich, soweit nicht das öffentliche Wohl oder die berechtigten Interessen Einzelner den Ausschluss der Öffentlichkeit erfordern (§ 64 NKomVG).

Das öffentliche Wohl kann die Beratung in nicht-öffentlicher Sitzung erfordern, zum Beispiel bei der Aussprache über:

- den Erwerb oder die Veräußerung von Grundstücken,
- Erschließungsabsichten,
- Angelegenheiten der Landesverteidigung.

Berechtigte Interessen Einzelner können zum Beispiel dann betroffen sein, wenn die Abgeordneten sich über:

- Personal- und insbesondere Disziplinarangelegenheiten,
- Stundungs- und Erlassgesuche von Abgabepflichtigen ,

- persönliche Angelegenheiten einer Bewerberin oder eines Bewerbers austauschen.

Die Verschwiegenheitspflicht gilt auch nach Beendigung der ehrenamtlichen Tätigkeit. Selbst für eine Aussage vor Gericht kann nur die Vertretung Befreiung von der Verschwiegenheitspflicht erteilen.

Wie verhält es sich nun aber konkret mit personenbezogenen Daten, von denen kommunale Abgeordnete Kenntnis erlangen? Und wie sind personenbezogene Daten überhaupt definiert?

In § 3 Abs. 1 NDSG heißt es:

„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen.“

Unter Angaben über die persönlichen Verhältnisse versteht man unter anderem folgendes:

- Namen,
- Geburtsdatum,
- Alter,
- Staatsangehörigkeit,
- Familienstand,

weitergehend aber auch persönliche Interessen wie die Weltanschauung oder den gesundheitlichen Zustand einer Person.

Zu den sachlichen Verhältnissen einer Person gehören z. B.:

- Informationen über Grundbesitz,
- Abgaben und Steuern,
- Versicherungen oder Bankguthaben.

Eine klare Trennung der Angaben zu den persönlichen Verhältnissen einerseits und den sachlichen Verhältnissen andererseits ist allerdings wegen vielfältiger Überschneidungen nicht möglich. Dies ist auch nicht erforderlich, da es sich ja in beiden Fällen um personenbezogene Daten handelt.

Das Datenschutzrecht findet aber auch bei personenbeziehbaren Daten Anwendung. Personenbeziehbar sind Daten, wenn durch ihre Nennung indirekt auf eine bestimmte Person geschlossen werden kann.

So viel zur Begriffsbestimmung der personenbezogenen Daten. Doch was gehen Abgeordnete die personenbezogenen Daten ihrer Mitbürgerinnen und Mitbürger an? Gemäß § 2 NDSG sind unter den Begriff der öffentlichen Stellen unter anderem Gemeinden, Landkreise oder die Region Hannover zu fassen, die gegebenenfalls personenbezogene Daten verarbeiten. Abgeordnete sind Teil einer Daten verarbeitenden öffentlichen Stelle!

Das Niedersächsische Datenschutzgesetz (NDSG) findet somit grundsätzlich auf die Tätigkeit als Abgeordnete Anwendung. Es gelten aber eine Reihe von spezialgesetzlichen Regelungen, die vorrangig anzuwenden sind (siehe § 2 Abs. 6 NDSG). Dies sind Bestimmungen aus dem NKomVG, z. B. über das Verfahren bei Angelegenheiten, die der Geheimhaltung unterliegen (§ 6 Abs. 3 NKomVG) oder zur Amtsverschwiegenheit (§ 40 NKomVG). Zudem gibt es das Sozialgeheimnis nach § 35 des Sozialgesetzbuches (SGB I Allgemeiner Teil), das Steuergeheimnis nach § 30 der Abgabenordnung (AO), Regelungen des Bundesmeldegesetzes (BMG) zu Melderegisterauskünften (§§ 44 ff BMG) oder spezielle Vorschriften zur Personaldatenverarbeitung nach dem Niedersächsischen Beamtenengesetz (§ 88 NBG).

Was müssen Abgeordnete aus datenschutzrechtlicher Sicht bei ihrer Mandatsausübung beachten?

Abgeordnete werden bei ihrer Tätigkeit in dem Gemeinderat, Stadtrat, Samtgemeinderat, Kreistag oder in der Regionsversammlung etc. immer wieder mit Situationen konfrontiert, in denen sie Kenntnis von personenbezogenen Daten erhalten. Nachfolgend habe ich einen Katalog von häufigen Fragestellungen aus der täglichen Praxis für kommunale Abgeordnete zusammengestellt. Ich möchte aber darauf hinweisen, dass dieser Fragenkatalog keinesfalls den Anspruch auf Vollständigkeit erhebt.

FRAGE 1: Wie kommen Sie als Abgeordnete bzw. Abgeordneter mit personenbezogenen Daten in Berührung?

Um über einen Sachverhalt entscheiden zu können, wird es immer wieder vorkommen, dass Ihnen personenbezogene Daten schriftlich, z. B. durch Verwaltungsvorlagen oder mündlich durch Erläuterungen und Diskussionen in Gremien, aber im Einzelfall auch telefonisch bekanntgegeben werden. Beinhalten die Sitzungsunterlagen personenbezogene Daten (z. B. bei Grundstücksangelegenheiten, im Zusammenhang mit Personalangelegenheiten oder bei Vergabeentscheidungen etc.), haben Sie einerseits den Persönlichkeitsschutz der Betroffenen zu wahren und andererseits der Notwendigkeit, auf aussagekräftige Entscheidungsunterlagen zurückgreifen zu können, Rechnung zu tragen.

FRAGE 2: Wie gelangen Sie an die für Ihre politische Arbeit notwendigen Informationen?

Die Verwaltung bereitet die Sitzungen durch die Aufstellung und öffentliche Bekanntmachung der Tagesordnung vor. Die Tagesordnung muss Ihnen als Ratsmitglied zugeleitet werden. Die Form der Übersendung kann in der Geschäftsordnung des Rates geregelt werden und unter Berücksichtigung moderner Medien (z. B. per E-Mail oder über ein Ratsinformationssystem) erfolgen. Die Verwaltung hat darauf zu achten, dass der Versand der Unterlagen in einer Form

erfolgt, die vor der Einsicht oder dem Zugriff Dritter geschützt ist (bei Papierversand sinnvollerweise: geschlossener Umschlag mit Hinweis auf Vertraulichkeit).

FRAGE 3: Wer darf Kenntnis von personenbezogenen Daten erhalten?

Hier gilt zunächst als oberstes Prinzip **der Grundsatz der Erforderlichkeit**. Kenntnis von personenbezogenen Daten dürfen nur diejenigen Personen oder Gremien erlangen, die für die Bearbeitung und Entscheidungsfindung der jeweiligen Angelegenheit zuständig sind.

FRAGE 4: Datenverarbeitung ist ein sehr komplexer Begriff. Was bedeutet er im Einzelnen?

Der Begriff Datenverarbeitung beinhaltet mehrere Komponenten, die in § 3 NDSG definiert sind. So ist

- Erheben: das Beschaffen von Daten,
- Speichern: das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger,
- Verändern: das inhaltliche Umgestalten von Daten,
- Übermitteln: das Bekanntgeben von Daten an Dritte,
- Sperren: das Kennzeichnen von Daten, um ihre weitere Verarbeitung einzuschränken,
- Löschen: das Unkenntlichmachen von Daten,
- Nutzen: jede sonstige Verwendung von Daten.

FRAGE 5: Was bedeutet das Datengeheimnis für Ihre politische Arbeit?

Das Datengeheimnis (§ 5 NDSG) verpflichtet Sie, personenbezogene Daten, zu denen Sie Zugang haben, nur zu dem Zweck zu verarbeiten, der für Ihre Aufgabenerfüllung vorgesehen ist. Geben Sie z. B. personenbezogene Daten, die Sie von der Verwaltung erhalten haben, an sogenannte Dritte (z. B. Bekannte, Partei etc.) weiter, so verstoßen Sie gegen § 5 NDSG. Sie hätten damit eine Ordnungswidrigkeit nach § 29 Abs. 1 NDSG begangen, die mit einer Geldbuße bis zu 50.000 Euro geahndet werden kann (§ 29 Abs. 2 NDSG). Im Einzelfall könnte es sich sogar um eine Straftat nach § 28 Abs. 1 NDSG handeln.

FRAGE 6: Was bedeutet Datensparsamkeit?

Datensparsamkeit ist ein essentieller Grundsatz im Datenschutzrecht. Es gilt die Devise „**So wenig wie möglich, so viel wie nötig**“, was die Datenmenge anbetrifft. Detailangaben sind oftmals nicht unbedingt erforderlich. So ist z. B.

- die Benennung einer genauen Adresse mit Straße und Hausnummer manchmal nicht nötig. Die Auskunft über den Wohnort kann ausreichend sein,

- das genaue Geburtsdatum oftmals nicht erforderlich; die Angabe des Alters in Jahren kann reichen,
- der Familienstand (ledig, geschieden, getrennt lebend) nicht immer anzugeben. Die Angabe "nicht verheiratet" kann genügen,
- bei Stellenbesetzungen die genaue Benennung von früheren und derzeitigen Arbeitgebern nicht vorzunehmen. Hier kann es ausreichen, die Art des Unternehmens oder die Branche anzugeben. Dies gilt insbesondere bei Bewerberinnen und Bewerbern in ungekündigter Stellung, die vielfach nicht wünschen, dass ihre Bewerbung dem derzeitigen Arbeitgeber bekannt wird.

FRAGE 7: *Im Zuge des Kommunalwahlkampfes möchten Sie sich als Kandidatin bzw. Kandidat für die Kommunalwahl personenbezogene Daten der älteren Mitbürgerinnen und Mitbürger in Ihrer Kommune von der Verwaltung geben lassen. Dürfen Sie das?*

Aus § 50 Abs. 1 Bundesmeldegesetz (BMG) geht folgendes hervor: „Die Meldebehörde darf Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene in den sechs der Wahl oder Abstimmung vorangehenden Monaten Auskunft aus dem Melderegister über die in § 44 Absatz 1 Satz 1 bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. Die Geburtsdaten der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. Die Person oder Stelle, der die Daten übermittelt werden, darf diese nur für die Werbung bei einer Wahl oder Abstimmung verwenden und hat sie spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten.“ Hieraus folgt, dass Ihre Partei oder Wählergruppe oder Sie selbst, sofern Sie Träger/in eines Wahlvorschlages sind (dies wäre der Fall, wenn Sie keiner Partei oder Wählergruppe angehören bzw. Ihr Handeln keiner Partei oder Wählergruppe zugeordnet werden kann), unter den zuvor genannten Voraussetzungen berechtigt sind, entsprechende Daten von Ihrer Meldebehörde anzufordern und zu Wahlwerbezwecken zu nutzen. Sofern Sie einer Partei oder Wählergruppe angehören, bestehen datenschutzrechtlich keine Bedenken, wenn Ihre Partei oder Wählergruppe Ihnen die von der Meldebehörde erhaltenen Daten der Personen übermittelt, die in Ihrem Wahlkreis wahlberechtigt sind.

Die Daten, die in § 44 Abs. 1 Satz 1 BMG genannt sind und von der Meldestelle an Ihre Partei, Wählergruppe oder an Sie als Träger/in eines Wahlvorschlages übermittelt werden dürfen sind folgende:

- Familienname,
- Vornamen,
- Doktorgrad und
- derzeitige Anschriften sowie,
- sofern die Person verstorben ist, diese Tatsache.

Diese sogenannte „Melderegisterauskunft in besonderen Fällen“ bezieht sich auf klar umgrenzte Bevölkerungsgruppen eines bestimmten Lebensalters. Es ist also unzulässig, wenn ein Verzeichnis der Bürgerinnen und Bürger „zwischen 16 und 100 Jahren“ angefordert wird. Damit bekäme man eine Aufstellung aller wahlberechtigten Bürgerinnen und Bürger der Kommune. Fordert man hingegen eine Liste aller Seniorinnen und Senioren über 60 Jahren an, so ist dies zulässig, da es sich um eine begrenzte Gruppe von Personen handelt.

Die Betroffenen haben im Übrigen nach § 50 Abs. 5 BMG das Recht, einer Übermittlung ihrer Daten an Parteien, Wählergruppen und andere Trägerinnen und Träger von Wahlvorschlägen zu widersprechen.

Ihre Partei oder Wählergruppe muss die Daten spätestens einen Monat nach der Wahl löschen oder an die Meldebehörde zurückgeben. Gleiches gilt für Sie, wenn Sie beispielsweise Daten von Ihrer Partei erhalten haben. Bitte nicht vergessen!

Eine Nutzung der Daten zu anderen Zwecken, z. B. zur Mitgliederwerbung oder ggf. zu einer anderen Wahl, ist **nicht zulässig**.

FRAGE 8: Können Sie außerhalb der Sechsmonatsfrist vor Wahlen mit Hilfe der sogenannten „Gruppenauskunft“ nach § 46 BMG Daten aus dem Melderegister bekommen?

Nein! Eine Gruppenauskunft darf nur erteilt werden, wenn sie im öffentlichen Interesse liegt. Unter öffentlichem Interesse ist vor allem das Interesse der Allgemeinheit zu verstehen, das über das Individualinteresse einzelner Personen oder Gruppen weit hinausgeht. Deshalb sind Gruppenauskünfte außerhalb der „Wahlkampfzeit“ an Parteien und Wählergruppen in aller Regel unzulässig – umso mehr gilt dies für Auskünfte an Sie als Einzelperson.

FRAGE 9: Wie verhält es sich bei Jubiläen?

Verlangen Mandatsträgerinnen und -träger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnerinnen und Einwohnern, darf die Meldebehörde gemäß § 50 Abs. 2 BMG Auskunft erteilen über:

- Familienname,
- Vornamen,
- Doktorgrad,
- Anschrift sowie
- Datum und Art des Jubiläums.

Altersjubiläen im Sinne des Satzes 1 sind der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 100. Geburtstag jeder folgende Geburtstag; Ehejubiläen sind das 50. und jedes folgende Ehejubiläum.

FRAGE 10: Dürfen Sie auch weitergehende Informationen über einzelne Personen einholen?

Die sogenannte erweiterte Melderegisterauskunft gemäß § 45 Abs. 1 BMG ist nur an Personen, die ein berechtigtes Interesse glaubhaft machen können, zulässig. Die Rechtsprechung hat ein berechtigtes Interesse definiert als „ein nach vernünftiger Abwägung durch die Sachlage gerechtfertigtes Interesse, das rechtlicher, wirtschaftlicher oder ideeller Natur sein kann und das von der Rechtsordnung anerkannt ist.“ Ein berechtigtes Interesse ist also nahezu jedes Interesse außerhalb der reinen Neugier.

Wenn Sie ein solches berechtigtes Interesse glaubhaft machen können, darf Ihnen die Meldebehörde folgende Daten **einer** bestimmten Person mitteilen:

- frühere Namen,
- Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,
- Familienstand, beschränkt auf die Angabe, ob verheiratet oder eine Lebenspartnerschaft führend oder nicht,
- derzeitige Staatsangehörigkeiten,
- frühere Anschriften,
- Einzugsdatum und Auszugsdatum,
- Familienname und Vornamen sowie Anschrift der gesetzlichen Vertreterin bzw. des gesetzlichen Vertreters,
- Familienname und Vornamen sowie Anschrift der Ehegattin bzw. des Ehegatten oder der Lebenspartnerin bzw. des Lebenspartners sowie
- Sterbedatum und Sterbeort sowie bei Versterben im Ausland auch den Staat.

Allerdings müssen Sie Ihr berechtigtes Interesse bezogen auf jedes einzelne der vorstehenden Daten glaubhaft machen, sonst darf Ihnen die Meldebehörde das Datum nicht mitteilen.

Die Meldebehörde hat die betroffene Person außerdem darüber zu informieren, dass sie Ihnen eine erweiterte Melderegisterauskunft erteilt hat!

FRAGE 11: Wie können behördliche Datenschutzbeauftragte (DSB) bei Fragen des Datenschutzes helfen?

DSB unterstützen die öffentlichen Stellen bei der Sicherstellung des Datenschutzes und wirken auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. Für die DSB gilt Weisungsfreiheit; sie können sich unmittelbar an die Behördenleitung wenden und dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden.

Jede öffentliche Stelle hat nach § 8 a NDSG eine bzw. einen DSB zu bestellen. Die Bestellung hat unabhängig von der Mitarbeiterzahl der öffentlichen Stelle zu erfolgen. Es ist auch möglich, dass z. B. mehrere kleinere Gemeinden eine gemeinsame bzw. einen gemeinsamen DSB bestellen. Ebenso kann die Aufgabe der bzw. des DSB auf einen externen Dienstleister (z. B. Kommunale Datenzentrale) übertragen werden. Die DSB wirken auf die Einhaltung der datenschutzrechtlichen Vorschriften in ihrer Behörde hin. Sie haben auch zu prüfen, ob bei der Verarbeitung personenbezogener

Daten die Grundsätze der Datenvermeidung und Datensparsamkeit eingehalten werden. Ferner obliegen ihnen u. a.

- die Beratung der Behördenleitung sowie einzelner Fachbereiche, Abteilungen und Ämter in Fragen des Datenschutzes und der Datensicherung,
- die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme,
- die Prüfung, ob die technischen Maßnahmen nach dem jeweiligen Stand der Technik getroffen sind, um die datenschutzrechtlichen Vorschriften sicherzustellen und
- die Schulung der mit der Verarbeitung personenbezogener Daten befassten Mitarbeiterinnen und Mitarbeiter.

Eine weitere wichtige Aufgabe der DSB besteht darin, dass sie auf der örtlichen Ebene als Ansprechpartnerin bzw. Ansprechpartner für Fragen des Datenschutzes zur Verfügung stehen. Artikel 37 Abs. 7 der ab Mai 2018 unmittelbar geltenden EU-Datenschutz-Grundverordnung (DSGVO) sieht daher die Veröffentlichung der Kontaktdaten der bzw. des DSB vor. Bürgerinnen und Bürger, die sich durch die öffentliche Stelle in ihrem Recht auf informationelle Selbstbestimmung verletzt fühlen, können sich direkt an die DSB wenden. Dasselbe gilt für die Bediensteten der Behörde.

Als Abgeordnete haben Sie allerdings keinen direkten Auskunftsanspruch gegenüber den DSB, sondern müssen sich bei den für Ihre Mandatsausübung notwendigen Fragen des Datenschutzes grundsätzlich an die Hauptverwaltungsbeamtin oder den Hauptverwaltungsbeamten (§ 56 NKomVG) wenden.

FRAGE 12: *Als Abgeordnete dürfen Sie bei allen Ausschusssitzungen anwesend sein, auch wenn Sie dem Ausschuss nicht angehören. Worin besteht in diesen Fällen Ihr Recht auf Information?*

Das Recht, an allen Sitzungen der Ratsausschüsse, egal ob diese in öffentlicher oder nicht-öffentlicher Sitzung tagen, zuhörend teilzunehmen, auch wenn Sie diesen nicht angehören, ergibt sich aus § 72 Abs. 2 NKomVG. Einen gesonderten Anspruch auf Informationen (insbesondere Beschlussvorlagen) für einzelne Abgeordnete, die dem Ausschuss nicht angehören, gibt es grundsätzlich nicht. Dieser Grundsatz wird nur dann außer Kraft gesetzt, wenn eine Abgeordnete bzw. ein Abgeordneter im Rat oder einem anderen Ausschuss einen Antrag gestellt hat und dieser Antrag nun in einem Ausschuss beraten werden soll, dem er nicht angehört. In diesem Sonderfall haben die Abgeordneten alle Mitgliedschaftsrechte zu dem entsprechenden Tagesordnungspunkt bis auf das Recht, an der Abstimmung teilzunehmen.

FRAGE 13: *Haben stellvertretende Ausschussmitglieder dieselben Rechte auf Information wie die ordentlichen Ausschussmitglieder?*

Im Verhinderungsfall übergibt das Ausschussmitglied die Sitzungsunterlagen üblicherweise an seine Vertreterin oder seinen Vertreter und erhält sie nach der Sitzung von diesen auch wieder zurück. Fällt ein Ausschussmitglied derartig

kurzfristig aus, dass es die Sitzungsunterlagen persönlich nicht mehr rechtzeitig an seine Vertretung weitergeben kann, so kann sich die Vertreterin oder der Vertreter die Unterlagen bei ihrer / seiner Fraktion besorgen. Der Fraktion steht immer ein kompletter Satz der jeweiligen Sitzungsunterlagen zur Verfügung. Soweit in Ihrer Behörde ein Ratsinformationssystem verwendet wird, können den Vertreterinnen und Vertretern im Vertretungsfall auch entsprechende Rollenberechtigungen eingeräumt werden.

FRAGE 14: *Bei Ihrer Kommune liegen Stellenbewerbungen vor, über die Sie als Mitglied des Hauptausschusses zu entscheiden haben. Welche Informationen über die Bewerberinnen und Bewerber dürfen Sie bekommen?*

Im Rahmen des Auswahlverfahrens hat die Verwaltung die datenschutzrechtlichen Grundsätze der Erforderlichkeit und der Datensparsamkeit zu beachten. D. h., dass sie nur die Daten aus den Bewerbungsunterlagen verarbeiten und an das für die Entscheidung zuständige Gremium weiterleiten darf, die für die jeweilige Entscheidungsfindung erforderlich sind. Maßgeblich sind dabei das in der Ausschreibung genannte Anforderungsprofil für den zu besetzenden Arbeitsplatz/Dienstposten unter Berücksichtigung der Kriterien der Bestenauslese (s. Artikel 33 Abs. 2 Grundgesetz). In der Praxis werden zu diesem Zweck oftmals Synopsen mit den relevanten Daten erstellt.

FRAGE 15: *Sind für die Änderung des Stellenplanes personenbezogenen Daten zu erheben?*

Eine Änderung des Stellenplans kommt grundsätzlich ohne die Erhebung personenbezogener Daten aus. Lediglich der Vollzug, also die konkrete Besetzung der Stelle, erfordert die Weitergabe von Personaldaten an das zuständige Gremium.

FRAGE 16: *Um mit der örtlichen Presse sachgerecht über die anstehende Neufestsetzung der Gewerbesteuerhebesätze diskutieren zu können, erbitten Sie sich eine betriebsbezogene Aufstellung, aus der Sie ersehen können, welche Gewerbebetriebe in welcher Höhe Gewerbesteuer zahlen. Darf Ihnen die Hauptverwaltungsbeamtin bzw. der Hauptverwaltungsbeamte diese Aufstellung zuleiten?*

Die Hauptverwaltungsbeamtin bzw. der Hauptverwaltungsbeamte darf Ihnen diese Aufstellung nicht zuleiten! In der Abgabenordnung (AO) wird das Steuergeheimnis besonders geschützt (§ 30 AO). Danach ist die Weitergabe der Daten im vorliegenden Fall nur dann möglich, wenn diese Daten für ein Verwaltungsverfahren benötigt werden. Allenfalls könnten **anonymisierte** Daten, so z. B. Zahlen über das Gesamtaufkommen an Gewerbesteuer der letzten Jahre, weitergegeben werden.

FRAGE 17: *Sie möchten im Rat einen Antrag stellen, dass sozial bedürftige Personen künftig geringere Eintrittsgelder für die städtischen Schwimmbäder zahlen. Um diesen Personenkreis gezielt über Ihren Antrag informieren zu können, erbitten*

Sie eine Adressliste der Sozialhilfeempfängerinnen und –empfänger Ihrer Stadt. Darf Ihnen die Hauptverwaltungsbeamtin bzw. der Hauptverwaltungsbeamte diese Liste aushändigen?

Nein! Die Daten dürfen nur mit Einverständnis der Betroffenen weitergegeben werden, da die Daten nicht zu dem Zweck verwendet werden sollen, für den sie erhoben wurden (Grundsatz der Zweckbindung). Zudem ist auch kein gesetzlicher Grund für die Datenweitergabe gegeben (§ 35 des SGB I in Verbindung mit § 67b SGB X). Das Ziel, die Betroffenen zu informieren, können Sie über die örtliche Presse, einen Wahlkampfstand oder Flugblätter erreichen.

FRAGE 18: *Darf ich während einer Ratssitzung fotografieren?*

Grundsätzlich dürfen während einer öffentlichen Gemeinderatssitzung Fotografien angefertigt werden. Voraussetzung ist, dass die Fotos offen und für jedermann erkennbar gemacht werden, die Fotografierten keine Einwände dagegen haben und die Fotos **nur mit dem Einverständnis** der fotografierten Personen weiter verwendet werden. Der ordnungsgemäße Ablauf der Sitzung darf zudem nicht gestört werden.

FRAGE 19: *Sind Tonbandaufzeichnungen der Protokollführerin bzw. des Protokollführers während der Ratssitzung erlaubt und wie verhält es sich generell datenschutzrechtlich mit Bild- und Tonaufzeichnungen von Sitzungen?*

Die Verwendung von Tonbändern zur ordnungsgemäßen Erstellung der Niederschrift ist nicht unumstritten. Dennoch geht die herrschende Rechtsauffassung davon aus, dass Tonbandaufzeichnungen als Hilfsmittel zur Erstellung der Niederschrift zulässig sind, insbesondere wenn die Vertretung dies in ihrer Geschäftsordnung ausdrücklich bestimmt hat (siehe Robert Thiele, Niedersächsisches Kommunalverfassungsrecht, 2011, § 68 Rn. 1). Wichtig ist in diesem Zusammenhang, dass die Tonbandaufzeichnung nach der Genehmigung der Niederschrift durch die Vertretung von der Verwaltung gelöscht wird. Bis zur Genehmigung der Niederschrift können die Abgeordneten die Tonbandaufzeichnungen abhören.

Einige Kommunen wollen gern im Rahmen einer bürgerfreundlichen und serviceorientierten Verwaltung öffentliche Sitzungen im Internet über ihre Homepage oder auf örtlichen TV-Sendern übertragen lassen. Hierzu ist allerdings zu sagen, dass es in Niedersachsen bislang an einer entsprechenden Rechtsgrundlage für die Aufzeichnung und Übertragung einer öffentlichen Sitzung via Bild- und Ton fehlt. Es ist daher erforderlich, dass für alle Bild- und Tonübertragungen die Einwilligungen einzuholen sind. Es besteht somit ein Zustimmungserfordernis für Bild- und Tonübertragung der Abgeordneten, sodass nur Bild- und Tonübertragungen von den Abgeordneten erfolgen dürfen, die vorab eingewilligt haben. Zudem dürfen keine Bild- und Tonübertragungen von den übrigen Anwesenden vorgenommen werden.

Von einem Live-Stream ohne zeitliche Verzögerung wird auch bei Vorliegen der Einwilligungen der Abgeordneten abgeraten, zumal nie auszuschließen ist, dass von übrigen Anwesenden Zwischenrufe erfolgen. Es ist beabsichtigt, mit der Novellierung

des NKomVG den § 64 zu erweitern und dort eine gesetzliche Regelung zu Film- und Tonaufnahmen von den Mitgliedern der Vertretungen aufzunehmen.

FRAGE 20: *Wie ist mit Sitzungsniederschriften zu verfahren?*

Gegen die Veröffentlichung von Verlaufs- oder Ergebnisprotokollen über öffentliche Sitzungen bestehen aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken. Wortprotokolle und Protokolle, die schützenswerte personenbezogene Daten beinhalten, sollten nur den tatsächlichen Sitzungsteilnehmerinnen und -teilnehmern bzw. in einem Exemplar den Fraktionen zugeleitet werden. Niederschriften nicht-öffentlicher Sitzungen sind nur denjenigen Abgeordneten zuzusenden, die an der Sitzung teilgenommen haben.

FRAGE 21: *Dürfen Sie Sitzungsunterlagen weitergeben?*

Nein! Das Weitergabeverbot von Unterlagen mit personenbezogenen Daten bezieht die Mitteilung des Inhaltes an Dritte mit ein. Dies gilt für mündliche und schriftliche Mitteilungen. Als Dritte einzustufen sind hier nicht nur beispielsweise Familienmitglieder, Kolleginnen und Kollegen, Bekannte, Nachbarinnen und Nachbarn, sondern auch Parteifreunde. Endet Ihr Mandat, so müssen Sie alle verbliebenen Unterlagen an die Verwaltung zurückgeben bzw. datenschutzgerecht vernichten.

Generell sind Sie als Abgeordnete verpflichtet, alle erhaltenen Unterlagen mit personenbezogenen Daten gegen die Kenntnisnahme oder den Zugriff Dritter zu sichern. Sitzungsunterlagen sind keine privaten Unterlagen, sondern ausschließlich für den Verwaltungsgebrauch bzw. Ihre Arbeit als Abgeordnete bzw. Abgeordneter bestimmt.

FRAGE 22: *Ein Journalist erbittet von Ihnen Informationen über eine nicht-öffentliche Sitzung des **Hauptausschusses**. Er verweist Sie darauf, dass nach dem Niedersächsischen Pressegesetz eine Auskunftspflichtung der Gemeinde besteht. Wie verhalten Sie sich?*

Sie sind als Abgeordnete bzw. Abgeordneter grundsätzlich nicht verpflichtet, dem Journalisten Auskünfte zu erteilen. Die grundsätzliche Auskunftspflichtung der Gemeinde hingegen gegenüber der Presse ergibt sich aus § 4 des Niedersächsischen Pressegesetzes. Danach sind die Behörden verpflichtet, den Vertreterinnen und Vertretern der Presse die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen. Sie können die Journalistin bzw. den Journalisten an die Hauptverwaltungsbeamtin bzw. den Hauptverwaltungsbeamten verweisen, da ihr bzw. ihm die Unterrichtung der Presse über Angelegenheiten der Gemeinde im Rahmen der Unterrichtungspflicht der Bevölkerung obliegt (§ 85 Abs. 5, 6 NKomVG), und sie bzw. er prüfen muss, ob es Gründe gibt, die Auskunft zu verweigern. Dies kann zum Beispiel gegeben sein, wenn mit der Erteilung der Auskunft ein überwiegendes öffentliches oder ein schutzwürdiges privates Interesse verletzt würde.

FRAGE 23: *Darf ich Notizen aus einer Gemeinderatssitzung veröffentlichen, z. B. im Internet?*

Zu öffentlichen Sitzungen des Gemeinderates hat grundsätzlich jedermann Zutritt. Den Zuhörerinnen und Zuhörern ist es gestattet, sich Notizen zu machen und daraus einen aus dem Gedächtnis verfassten Bericht z. B. im Internet zu veröffentlichen. Das gilt auch für Sie als Abgeordnete, sofern sich Ihre Veröffentlichung auf diejenigen Vorgänge beschränkt, die nicht der Amtsverschwiegenheit und dem Datengeheimnis unterliegen. Bei Ihrer Publikation muss jedoch klar erkennbar sein, dass es sich um persönliche Aufzeichnungen handelt und nicht um eine Veröffentlichung der Gemeinde oder eine amtliche Niederschrift.

FRAGE 24: *Was passiert mit personenbezogenen Daten, wenn Sie diese für Ihre Mandatstätigkeit nicht mehr benötigen, weil der Vorgang abgeschlossen ist?*

Personenbezogene Daten sind unverzüglich zu löschen bzw. zu vernichten, wenn sie nicht mehr erforderlich sind. Ihre Arbeit als Abgeordnete bzw. Abgeordneter wird durch die Datenvernichtung nicht beeinträchtigt, weil Sie als Gremienmitglied bei Bedarf jederzeit im Rahmen Ihrer Zuständigkeiten auf die archivierten Dokumente bei der Verwaltung oder ihrer Fraktion zurückgreifen können.

FRAGE 25: *Gibt es Mindestanforderungen für die Vernichtung von Unterlagen?*

Dokumente, die personenbezogene Daten enthalten, dürfen keinesfalls über den Hausmüll oder die Altpapierabholung entsorgt werden. Auch das Zerreißen oder das einfache „In-Streifen-Schneiden“ (Schreddern) von Papierseiten ist meist nicht ausreichend. Bei elektronischen Datenträgern, wie z. B. USB-Sticks, CDs, DVDs oder Festplatten ist besondere Vorsicht geboten. Sie dürfen niemals ohne die vorherige datenschutzgerechte, unwiderrufliche Löschung der auf ihnen enthaltenen personenbezogenen Daten entsorgt werden. Die Löschung der Daten muss dergestalt erfolgen, dass eine spätere Wiederherstellung der Daten ausgeschlossen ist.

Weiterführende Informationen zur Vernichtung und Löschung finden Sie im Internet unter www.lfd.niedersachsen.de, Menüpunkt „Technik und Organisation / Orientierungshilfen und Handlungsempfehlungen / Vernichtung und Löschung“. In diesem Zusammenhang erfolgt hier der Hinweis auf die DIN-Norm zur Datenträgervernichtung DIN 66399.

Beim Einsatz mobiler Datenträger empfehle ich, Systeme mit zusätzlichen Schutzmechanismen (z.B. Verschlüsselung) zu verwenden, damit im Falle des Verlustes die Finderin bzw. der Finder nicht auf die gespeicherten Daten zugreifen kann.

FRAGE 26: *Dürfen Daten von Abgeordneten durch die Verwaltung bekannt gegeben werden?*

Veröffentlicht eine Kommune in ihren Publikationsorganen die Zusammensetzung der Gremien mit näheren Angaben zu den Mitgliedern, so ist dagegen nichts einzuwenden, wenn sich die Angaben auf diejenigen persönlichen Daten beschränken, die anlässlich der Kommunalwahl öffentlich bekannt gemacht worden sind.

FRAGE 27: *Dürfen Sie in die über Sie gespeicherten Daten bei der Verwaltung Einsicht nehmen?*

§ 16 NDSG regelt die Auskunfts- und Akteneinsichtsrechte der Betroffenen. Die Daten verarbeitende Stelle muss Ihnen auf Antrag Auskünfte erteilen über die zu Ihrer Person gespeicherten Daten. Auch der Zweck und die Rechtsgrundlage der Speicherung sowie die Herkunft der Daten und die Empfängerinnen und Empfänger von eventuellen Übermittlungen müssen Ihnen bekannt gegeben werden. Dieser Auskunftsanspruch ist ein wesentlicher Bestandteil Ihres Rechts auf informationelle Selbstbestimmung.

Der Antrag auf Auskunft ist form- und fristlos, sinnvollerweise aber schriftlich zu stellen. Die Auskunft und die Akteneinsicht sind kostenlos.

FRAGE 28: *Kann Ihnen die Auskunft verweigert werden?*

Die Auskunft kann verweigert werden, wenn die Auskunftserteilung den ordnungsgemäßen Arbeitsablauf der Daten verarbeitenden Stelle beeinträchtigt. Des Weiteren darf die öffentliche Sicherheit nicht gefährdet werden, und dem Bund und den Ländern dürfen keine Nachteile entstehen. Ein dritter Hinderungsgrund der Auskunftserteilung besteht darin, dass die personenbezogenen Daten auf Grund einer Rechtsvorschrift oder wegen berechtigter Interessen Dritter geheim zu halten sind (§ 16 Abs. 4 NDSG).

FRAGE 29: *Können Sie die Verarbeitung Ihrer personenbezogenen Daten verhindern?*

§ 17a NDSG sieht ein Widerspruchsrecht für Betroffene vor. Wenn also schutzwürdige persönliche Gründe vorliegen, können Sie bei der Daten verarbeitenden Stelle Widerspruch gegen die Verarbeitung Ihrer Daten einlegen. Überwiegen Ihre persönlichen Gründe das Interesse der öffentlichen Stelle an der Datenverarbeitung, so ist die Verarbeitung unzulässig.

Das Widerspruchsrecht gilt nicht, wenn eine Rechtsvorschrift die Datenverarbeitung verpflichtend vorsieht.

FRAGE 30: *Wie werden Verstöße gegen das Datenschutzrecht geahndet?*

Wer personenbezogene Daten, die nicht allgemein zugänglich sind, entgegen der Zweckbindung verarbeitet, offenbart (siehe hierzu auch § 5 NDSG), sich durch

Vortäuschung falscher Tatsachen verschafft oder an sich oder andere übermitteln lässt, handelt ordnungswidrig. Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50.000 Euro belegt werden (siehe § 29 NDSG).

Strafbar macht sich sogar, „wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, personenbezogene Daten, die nicht allgemein zugänglich sind,

1. unbefugt erhebt, speichert, verändert, löscht, übermittelt oder nutzt oder
2. durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst.“

Auch der Versuch ist strafbar. Ein Verstoß wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe geahndet (§ 28 NDSG).

FRAGE 31: *Aufgrund von wiederholt aufgetretenen Sachbeschädigungen an öffentlichen Gebäuden möchte die Verwaltung eine Videoüberwachungsanlage installieren. Darf sie das?*

Nach § 25a NDSG dürfen öffentlich zugängliche Bereiche grundsätzlich durch Bildübertragung (Videoüberwachung) beobachtet werden. Bevor die Überwachungstechnik aber eingesetzt wird, ist eine Vielzahl von Formvorschriften zu beachten. So muss z. B. dem Einsatz von Videoüberwachungstechnik immer eine Prüfung nach § 7 Abs. 3 NDSG, die sogenannte Vorabkontrolle, vorausgehen (§ 25a Abs. 6). Sofern Mitarbeiterinnen und Mitarbeiter der öffentlichen Stelle von der Videobeobachtung betroffen sind, darf keine Verhaltens- und Leistungskontrolle stattfinden. Das gilt auch für das Betreten und das Verlassen des Grundstücks bei Dienstbeginn bzw. Dienstende. Beim Einsatz von Überwachungstechnik in Schulen gelten besondere und strengere Voraussetzungen! So trägt z. B. die Schulleitung gem. § 43 Niedersächsisches Schulgesetz (NSchG) die Gesamtverantwortung und ist somit für alle an der Schule tätigen Personen und die Schülerinnen und Schüler verantwortlich. Sie ist daher immer mit einzubinden. Bei der Einführung von Videoüberwachungstechnik handelt es sich zudem um eine wesentliche Angelegenheit i. S. v. § 34 Abs. 3 NSchG, über die die Gesamtkonferenz durch die Schulleitung entsprechend zu unterrichten ist.

Ich habe zur Videoüberwachung unter anderem die folgenden Orientierungshilfen erarbeitet:

- „Orientierungshilfe zur Videoüberwachung durch öffentliche Stellen im Land Niedersachsen“
- „Orientierungshilfe zur Videoüberwachung an öffentlichen Schulen“

Beide Ratgeber sind im Internet unter <http://www.lfd.niedersachsen.de>, Menüpunkt „Themen/ Videoüberwachung“ zum Download verfügbar. Die Orientierungshilfe „Videoüberwachung von Arbeitsplätzen“ finden Sie ebenfalls auf meiner Homepage unter dem Menüpunkt „Themen/ Personaldatenschutz“.

4. Ratsinformationssysteme

Ein Bürger- bzw. Ratsinformationssystem (RIS) ist ein EDV-gestütztes Informations- und Dokumentationssystem, das bereits von den meisten Landkreisen, Städten und Gemeinden eingesetzt wird. RIS sind geeignet, auf automatisiertem Wege die Arbeit der politischen Organe der Kommune bis tief hinein in die Verwaltungsabläufe zu unterstützen.

Das RIS ermöglicht es sowohl den Abgeordneten als auch den Bürgerinnen und Bürgern, sich zeitnah über die politischen Beratungen und Entscheidungen in der Kommune zu informieren. So ist es häufig schon gängige Praxis, dass nicht nur die Tagesordnung der kommunalen Gremien, sondern auch bereits die zur Beratung und Beschlussfassung anstehenden Vorlagen sowie die Niederschriften der Sitzungen ins kommunale Internetangebot eingestellt werden.

Für die datenschutzgerechte Nutzung von RIS verweise ich auf meine Handreichung: „Empfehlungen für den datenschutzgerechten Einsatz von Ratsinformationssystemen“. Sie finden diese in meinem Internetangebot unter: <http://www.lfd.niedersachsen.de>, Menüpunkt „Themen/ Kommunales/ Ratsinformationssysteme“.

5. Sicherer Einsatz technischer Geräte in der Gremienarbeit

Datensicherheit umfasst die Summe aller technischen und organisatorischen Sicherungsmaßnahmen, die erforderlich sind, um eine den Datenschutznormen entsprechende Datenverarbeitung sicher zu stellen. Kommen in der Gremienarbeit technische Geräte zur Verarbeitung personenbezogener Daten zum Einsatz, sind die erforderlichen Maßnahmen zur Datensicherheit nach § 7 NDSG zu treffen.

Stellt die Verwaltung den Abgeordneten die für ihre Tätigkeit vertraulichen Daten optimalerweise über ein Ratsinformationssystem zur Verfügung, trägt sie die Verantwortung für dessen datenschutzgerechte Ausgestaltung.

Soweit mobile Endgeräte (z. B. Notebooks oder Tablets) für die Gremienarbeit zum Einsatz kommen, birgt dies immer auch die Gefahr zusätzlicher Sicherheitslücken. Einen wertvollen Beitrag zur Datensicherheit können Kommunen daher leisten, indem sie den Abgeordneten sichere und datenschutzkonform ausgestaltete Systeme zur Verfügung stellen. Die Bereitstellung und Administration der mobilen Endgeräte obliegt dann der Kommune.

Bedingt durch die Vielfalt möglicher Betriebssysteme, die Notwendigkeit des Vorhaltens und der aktuellen Konfiguration komplexerer Sicherheitsanwendungen (Firewall, Virenschutz, Verschlüsselung etc.) und ständig wechselnde Angriffsszenarien auf Soft- und Hardwareschwächen sind der Erfahrung nach nur wenige Nutzerinnen und Nutzer mobiler Endgeräte selbst in der Lage diese hinreichend sicher zu administrieren. Der Einsatz privater Systeme sollte daher aus datenschutzrechtlicher Sicht nur erfolgen, wenn sich der Architekturansatz dadurch auszeichnet, dass private Endgeräte lediglich als Web-Endgerät genutzt werden und gewährleistet ist, dass die Datenhaltung (Speicherung, Transformation,

Nutzersteuerung durch Rechte-Kontrollen-Konzepte usw.) ausschließlich auf einem gesicherten Server der Kommune (oder einer beauftragten Stelle im Sinne des § 6 NDSG) und nicht lokal auf dem mobilen Endgerät erfolgt. Die Nutzung des privaten Endgerätes würde somit lediglich als Terminal für die Ein- und Ausgabe genutzt.

Soweit Abgeordnete für Ihre Gremienarbeit vertrauliche Daten auf einem privaten Endgeräte verarbeiten, gebe ich zu bedenken, dass die Verantwortung für deren Sicherheit und Integrität auf die jeweiligen Abgeordneten übergeht. Die Abgeordneten wären dann selbst in der Pflicht, die erforderlichen Maßnahmen zur Datensicherheit nach § 7 NDSG zu treffen.

6. Weiterführende Links

<http://www.lfd.niedersachsen.de/>

Der Internetauftritt der Landesbeauftragten für den Datenschutz Niedersachsen ist die erste Adresse für kommunale Mandatsträgerinnen und Mandatsträger in Niedersachsen. Die jeweils zuständigen Ansprechpartnerinnen und Ansprechpartner finden Sie im Menüpunkt „Wir über uns/ Ihre Ansprechpartner.“

<http://www.bfdi.de>

Das Internetportal der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bietet unter anderem eine Auswahl von Gesetzen und Urteilen, auch zum europäischen und internationalen Datenschutzrecht.

<http://www.datenschutz.de>

Das „virtuelle Datenschutzbüro“ stellt eine Vielzahl von Informationen zur Verfügung und zeichnet sich durch eine umfassende Beratungsfunktion aus.

<http://www.youngdata.de/>

„Youngdata“ ist das Jugendportal der unabhängigen Datenschutzbehörden des Bundes und der Länder, sowie des Kantons Zürich. Hier findet man Informationen zum Datenschutz und zur Informationsfreiheit, Tipps für ein kluges Verhalten im Internet und Berichte über die digitale Zukunft unserer Gesellschaft.

<http://www.bsi.de>

Das Portal des Bundesamtes für Sicherheit in der Informationstechnik informiert hauptsächlich zu allen technischen Themen.

<https://www.thm.de/zaftda/>

ZAfTDa ist das Zentralarchiv für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten sowie der Aufsichtsbehörden für den Datenschutz.

7. Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD)

Aufgabe der Landesbeauftragten für den Datenschutz ist es, die Einhaltung der datenschutzrechtlichen Vorschriften im öffentlichen und im nichtöffentlichen Bereich zu überwachen und so das Recht auf informationelle Selbstbestimmung zu sichern.

Die Landesbeauftragte für den Datenschutz überwacht, dass die öffentliche Verwaltung beim Umgang mit personenbezogenen Daten Gesetz und Recht einhält. Schwerwiegende Verstöße gegen das Datenschutzrecht durch die Landesverwaltung werden gegenüber der zuständigen obersten Landesbehörde, bei Gemeinden, Landkreisen und sonstigen der Aufsicht des Landes unterstehenden Stellen gegenüber dem vertretungsberechtigten Organ beanstandet. In aller Regel finden jedoch zunächst Gespräche mit der betroffenen Stelle statt, in denen versucht wird, datenschutzgerechtes Verhalten bzw. die Beseitigung von Mängeln durchzusetzen. Dies ist in den meisten Fällen erfolgreich, so dass von dem förmlichen Mittel der Beanstandung in der Praxis nur sehr selten Gebrauch gemacht werden muss.

Die Landesbeauftragte für den Datenschutz legt dem Landtag jeweils für zwei Kalenderjahre einen Tätigkeitsbericht vor. Der Bericht spiegelt die rechtlichen und technologischen Entwicklungen der letzten zwei Jahre sowie die zukünftigen Herausforderungen des Datenschutzes wieder und zeigt den datenschutzpolitischen Handlungsbedarf auf. Die Landesregierung nimmt hierzu gegenüber dem Landtag innerhalb von sechs Monaten Stellung.

Als Hilfestellung für die öffentlichen Stellen und zur Orientierung für die Bürgerinnen und Bürger hält die Landesbeauftragte für den Datenschutz auf ihrer Internetseite zahlreiche Informationen zu datenschutzrechtlichen Problemstellungen bereit und bietet Handlungsanleitungen und Orientierungshilfen unterschiedlichster Art an, die den datenschutzgerechten Umgang mit personenbezogenen Daten erleichtern sollen.

Besuchsadresse:

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover

Telefon: +49-0511-120-45 00
Telefax: +49-0511-120-45 99
E-Mail: poststelle@lfd.niedersachsen.de

Postfachadresse:

Die Landesbeauftragte für den Datenschutz Niedersachsen
Postfach 2 21
30002 Hannover