Landesbeauftragter für den Datenschutz Niedersachsen

Empfehlungen für den datenschutzgerechten Einsatz von Ratsinformationssystemen

I. Allgemeines/Grundsätzliches

In einer Vielzahl niedersächsischer Kommunen werden mittlerweile automatisierte Rats- oder Kreistagsinformationssysteme eingesetzt, die es der Verwaltung ermöglichen, den kommunalen Sitzungsdienst effizient zu steuern, es gleichzeitig den ehrenamtlichen Mandatsträgern und den Bürgerinnen und Bürgern ermöglichen, sich zeitnah über die in den kommunalen Gremien zur Beratung oder Beschlussfassung anstehenden Themen zu informieren. So werden vielfach schon nicht nur die Tagesordnung der kommunalen Gremien, sondern auch bereits die zur Beratung und Beschlussfassung anstehenden Vorlagen sowie die Niederschriften der Sitzungen in das einer breiten Öffentlichkeit zugängliche kommunale Internetangebot eingestellt.

In den kommunalen Vertretungskörperschaften und Ausschüssen werden jedoch vielfach im Rahmen der Beschlussfassung und Beratung auch schützenswerte und vertrauliche Angelegenheiten behandelt, so etwa im Zusammenhang mit der Beschlussfassung über Personalangelegenheiten, Auftragsvergaben, Vermietung oder Verpachtung kommunaler Einrichtungen, Vertragsangelegenheiten, der Festsetzung kommunaler Abgaben und Gebühren sowie über Anregungen und Beschwerden der Bürgerinnen und Bürger im Rahmen der Bauleitplanung.

II. Chancen und Risiken

Der Einsatz automatisierter Rats- oder Kreistagsinformationssysteme steigert ohne Zweifel die Effizienz der Aufgabenerledigung der kommunalen Verwaltungen in der Vor- und Nachbereitung der Sitzungen. Die Verfahren unterstützen darüber hinaus die ehrenamtliche Tätigkeit der Mandatsträger durch umfangreiche Recherche- und Archivfunktionen. Gleichzeitig erhöhen derartige Informationsangebote auch die Transparenz der Entscheidungen, die gerade auf kommunaler Ebene das persönliche Lebensumfeld der Bürgerinnen und Bürger vielfach unmittelbar berühren.

Da jedoch die modernen Informations- und Kommunikationstechniken vielfältige Möglichkeiten bieten, personenbezogene Daten zielgerichtet auszuwerten und zu verarbeiten, kann sich durch eine unzulässige Veröffentlichung im Internet und mangelnde Datensicherheit der in den Ratsinformationssystemen verarbeiteten und gespeicherten personenbezogenen Daten eine Gefährdung des Rechts auf informationelle Selbstbestimmung der Betroffenen ergeben.

III. Handlungsbedarf

Die Erfahrungen zeigen, dass in der konkreten Anwendung der Verfahren vor Ort in den Kommunen vielfach Unsicherheiten bestehen, insbesondere zu der Frage, wem Zugriff auf die in den Systemen gespeicherten personenbezogenen Daten gewährt werden darf, welche personenbezogenen Daten in Ratsinformationssystemen veröffentlicht werden dürfen und welche technisch-organisatorischen Maßnahmen zum Schutz der in den Ratsinformationssystemen verarbeiteten Daten zu treffen sind.

Auf Seiten der Bürgerinnen und Bürger sowie bei den Mandatsträgern wird die notwendige Akzeptanz für Ratsinformationssysteme jedoch nur zu erreichen sein, wenn die Vertraulichkeit und Integrität der in den Ratsinformationssystemen verarbeiteten personenbezogenen Daten gewahrt bleibt. Die nachstehenden Empfehlungen, die im Einvernehmen mit den kommunalen Spitzenverbänden und unter Mitwirkung niedersächsischer Kommunen entwickelt wurden, die schon seit längerem Rats- oder Kreistagsinformationssysteme einsetzen, soll den Verwaltungen und Mandatsträgern eine Hilfestellung bei der konkreten Ausgestaltung und Anwendung der Ratsinformationssysteme liefern.

IV. Informationsinteresse der Öffentlichkeit und Datenschutz

a) Nach § 64 des Niedersächsischen Kommunalverfassungsgesetzes (NKomVG) sind die Sitzungen des Rates grundsätzlich **öffentlich**. Hiervon abweichend sind Angelegenheiten, die aufgrund des öffentlichen Wohls oder **berechtigter Interessen einzelner** den **Ausschluss der Öffentlichkeit** erfordern, in **nichtöffentlicher Sitzung** zu behandeln. Berechtigte Interessen einzelner sind immer dann betroffen, wenn **vertrauliche und schützenswerte personenbezogene Daten** erörtert werden.

b) Datenschutzrechtlich ist die **Einsichtnahme in personenbezogene Sitzungsvorlagen** öffentlicher Sitzungen über das **Internet** als **Abruf aus Datenbeständen**, die jeder Person offen stehen oder deren Inhalt veröffentlicht werden darf, zu bewerten. Gemäß § 12 Abs. 5 des Niedersächsischen Datenschutzgesetzes (NDSG) finden bei einem Abruf aus solchen Datenbeständen die Regelungen des § 12 Abs. 1 bis 4 NDSG über die Zulässigkeit der Einrichtung und Ausgestaltung **automatisierter Abrufverfahren** keine Anwendung.

c) Letztlich bleibt es also dem Rat überlassen, darüber zu entscheiden, ob er es im Sinne der Bürgerfreundlichkeit, zur Verbesserung der Information und Erhöhung der Transparenz für angezeigt hält, die Tagesordnung, die Sitzungsvorlagen und die Niederschriften öffentlicher Sitzungen in das Internet einzustellen. Die Veröffentlichung sollte auf der Grundlage einer

entsprechenden **Beschlussfassung des Rates** und ergänzender Regelungen, die auch in der **Geschäftsordnung** getroffen werden können, erfolgen.

V. Nichtöffentliche Vorgänge und Amtsverschwiegenheit

a) Vorgänge, die aufgrund berechtigter Interessen der Betroffenen in nichtöffentlicher Sitzung zu behandeln sind, dürfen ohne das vorherige Einverständnis *(Einwilligung)* der Betroffenen einer breiten Öffentlichkeit nicht zugänglich gemacht werden. **Ihre Veröffentlichung im öffentlich zugänglichen Teil eines Ratsinformationssystems ist daher nicht zulässig.**

b) Derartige Vorgänge unterliegen auch der für ehrenamtliche Mandatsträger geltenden **Amtsverschwiegenheit** nach § 40 NKomVG.

c) Darüber hinaus sollten die Mandatsträger im Rahmen ihrer Verpflichtung auf ihre Rechte und Pflichten beim Umgang mit den Ratsinformationssystemen in besonderer Weise hingewiesen werden.

VI. Gestaltung der Inhalte von Ratsinformationssystemen

a) In Ratsinformationssystemen dürfen personenbezogenen Daten grundsätzlich nur verarbeitet werden, sofern dies für eine angemessene Information der Mandatsträger über den zur Beratung anstehenden Sachverhalt oder zur Unterrichtung der Einwohnerinnen und Einwohner erforderlich ist (Grundsatz der **Erforderlichkeit sowie der Datenvermeidung und Datensparsamkeit**).

b) Die **Tagesordnung** und die hierzu erstellten **Sitzungsvorlagen** sind daher inhaltlich grundsätzlich so zu gestalten, dass ein Personenbezug oder eine Personenbeziehbarkeit ausgeschlossen ist **(Anonymisierung oder Pseudonymisierung).** Dies gilt insbesondere, wenn die Angelegenheit in öffentlicher Sitzung zu behandeln ist.

   Beispiel: Einladung zur öffentliche Sitzung des Rates XY

   Top 7 : Beschwerden und Anregungen;
   Beschwerde eines Anwohners der K 217 aus dem Ortsteil Musterhausen über mangelhafte Straßenreinigung

c) Bereits bei der Erstellung der Vorlagen ist von den verantwortlichen Beschäftigten festzulegen, ob die Sitzungsvorlage und ergänzende Unterlagen in den öffentlichen Teil des Ratsinformationssystems eingestellt werden sollen oder nur den Nutzern zugänglich gemacht werden dürfen, die verwaltungsintern oder als Mandatsträger Zugriff auf den nichtöffentlichen Teil des Ratsinformationssystems haben. Die Festlegung ist im Bearbeitungsgang und abschließend vor der Freigabe einer Vorlage für den öffentlichen Teil erneut zu bewerten.

d) Die Veröffentlichung von **Niederschriften** von öffentlichen Sitzungen kommunaler Gremien ist auch ohne vorherige Einwilligung der Betroffenen grundsätzlich zulässig. Die Niederschriften sollten inhaltlich jedoch datenschutzgerecht gestaltet werden, d.h. personenbezogene Angaben nur dann in die Niederschriften aufgenommen werden, wenn dies im Einzelfall zur Dokumentierung des Beschlusses erforderlich ist. So sollte davon abgesehen werden, Wortprotokolle und Protokollierungen des Abstimmungsverhaltens einzelner Ratsfrauen oder Ratsherren in das Internet einzustellen.

VII. Zugriffs- und Einsichtsrechte

a) In der Verwaltung dürfen Vorlagen mit personenbezogenen Informationen, die in nichtöffentlicher Sitzung zu behandeln sind, nur den Beschäftigten zugänglich gemacht werden, die **im Rahmen ihrer Aufgabenerfüllung** an der Erstellung der Sitzungsunterlage und nachfolgenden Umsetzung der Beratungsergebnisse beteiligt sind (§ 11 Abs. 4 i.V.m. § 11 Abs. 1 NDSG).

b) Die **Zugriffs- und Einsichtsrechte** sind auf die jeweils übertragenen Aufgaben einzugrenzen **(Grundsatz der Zweckbindung).** Für den Zugriff auf das Verfahren und die Einsichtsrechte der Beschäftigten ist daher ein nach Schreib- und Leserechten differenziertes **Berechtigungskonzept** bzw. **Rollenprofil** zu erstellen.

   Beispiel:

   Auf eine Sitzungsvorlage für den Verwaltungsausschuss zur Besetzung einer Beförderungsstelle dürfen nur die Beschäftigten Zugriff nehmen, die mit der Bearbeitung der Personalangelegenheit befasst sind, in der Regel also die Mitarbeiter des Personalamtes.

c) Den **Mandatsträgern** darf ein Zugriff auf sämtliche Vorlagen auch nichtöffentlicher Sitzungen des Rates und der sonstigen Ausschüsse und Gremien eröffnet werden, auch wenn sie diesen Ausschüssen nicht angehören.

d) Mitglieder kommunaler Ausschüsse, die nicht Mitglied des Rates sind, dürfen nur auf die Vorlagen und Niederschriften nichtöffentlicher Sitzungen des Ausschusses zugreifen, dem sie angehören.

e) **Mitarbeitern von Fraktionen und Gruppen**, die selbst nicht Beschäftigte der Gemeinde sind, darf gemäß § 57 Abs. 4 NKomVG ein Zugriff auf vertrauliche Inhalte des Ratsinformationssystems nur eröffnet werden, wenn sie vorab durch den Bürgermeister nach dem **Verpflichtungsgesetz** zur Verschwiegenheit verpflichtet wurden.

VIII. Technisch-organisatorische Maßnahmen

Vor der Einführung, Anwendung oder einer nachhaltigen Veränderung eines Ratsinformationssystems ist eine **Vorabkontrolle** (früher „Technikfolgenabschätzung“) durchzuführen (§ 7 Abs. 3 NDSG). Dies auf der Grundlage einer **Verfahrensbeschreibung** nach § 8 NDSG.

Auf der Grundlage dieser Vorabkontrolle ist ein detailliertes **Sicherungskonzept** zu erstellen, das die notwendigen Maßnahmen zur Wahrung der **Sicherungsziele** Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit und ihre Realisierung im Einzelnen umfassend darstellt.

Im Folgenden werden beispielhaft einige Bereiche dargestellt, die in einem Sicherungskonzept stets zu behandeln sein werden.

a) Information, Dokumentation und Schulung

aa) Das Ratsinformationssystem ist umfassend zu dokumentieren; die genutzten Funktionalitäten sind transparent und verständlich darzustellen und in ihrer Bedienung allgemeinverständlich zu beschreiben. Die Nutzer des Systems sind in die Bedienung einzuweisen; dabei ist auf mögliche Gefahren und Risiken sowie auf praktikable Möglichkeiten ihrer Reduzierung einzugehen.

ab) Art und Umfang der Nutzung des Ratsinformationssystems sind verbindlich und für die Beschäftigten der Verwaltung nachvollziehbar in einer Dienstanweisung oder Dienstvereinbarung zu regeln.

ac) Die Verwaltung als Betreiberin des RIS ist verpflichtet, die Mandatsträger über die einzuhaltenden technisch-organisatorischen Maßnahmen zu informieren sowie diejenigen technisch-organisatorischen Voraussetzungen zu schaffen, die den Mandatsträgern einen sicheren Umgang mit dem RIS ermöglichen. Nicht in die Verantwortung der Verwaltung fallen Verhaltens- und Verfahrensweisen der Mandatsträger, die von den technisch-organisatorischen Vorgaben der Verwaltung abweichen bzw. die die Verwaltung nicht beeinflussen kann.

b) **Authentisierung und Rechteverwaltung**

ba) Für die Gesamtanwendung ist eine hinreichende Nutzerauthentisierung sowie ein durchgreifendes Rechtekonzept zu entwickeln und technisch umzusetzen. Dabei ist sicherzustellen, dass nur Nutzer Zugang zu dem System erhalten, die sich in geeigneter Weise beim System angemeldet haben und deren Berechtigung zweifelsfrei festgestellt worden ist.

bb) Durch geeignete Vergabe von Zugriffsrechten ist sicherzustellen, dass Nutzer nur die Inhalte einsehen können, für die sie zugelassen worden sind und nur Veränderungen an den Dokumenten vornehmen können, die ihren Aufgaben- oder Zuständigkeitsbereich umfassen. Die Umsetzung dieses Rechtekonzepts ist durch geeignete Maßnahmen sicherzustellen und stichprobenartig zu überwachen.

bc) Die Nutzung des Systems erfolgt stets mit Standardrechten; administrative Aufgaben bleiben speziellen Kennungen vorbehalten. Die Administration des Systems erfolgt durch qualifiziertes Personal; administrative Zugriffe, insbesondere soweit sie Änderungen an bestehenden Rechtekonzepten umfassen, werden nachvollziehbar protokolliert.

c) **Absicherung der Datenübertragung**

ca) Soweit Nutzern der Zugriff auf das System von Stellen außerhalb des lokalen Netzwerkes gewährt wird, ist eine gesicherte Übertragung der Daten über die externen Verbindungen sowie ein kontrollierter Zugang in das lokale Netzwerk zu gewährleisten. Als technische Mittel kommen hierfür insbesondere eine Verschlüsselung der Datenübertragung und die Absicherung des lokalen Netzes durch den Einsatz von geeigneter Firewall-Technologie in Betracht.

cb) Entsprechende Maßnahmen sind bei der Nutzung von e-Mail Diensten zu ergreifen; auch hier kommt im wesentlichen die Verschlüsselung in Betracht.

cc) Wird die Authentifikation der Nutzer mit Hilfe von Chipkarten-Systemen vorgenommen, sollte die Nutzung dieser Systeme für den Einsatz der digitalen Signatur sowie der Verschlüsselung vorgesehen werden.

d) **Speicherung von Daten aus dem System auf privaten PC**

da) Sofern Mandatsträger mit eigenen PC/Laptops von außerhalb auf das System zugreifen und Informationen aus dem System lokal speichern, sollte den Mandatsträgern angeboten werden, ihre PC/ Laptops vor der Nutzung von den Systemadministratoren der Verwaltung auf Sicherheitsmängel überprüfen zu lassen. Auf den PC/Laptops ist ein Vi-

renscanner einzusetzen, der regelmäßig aktualisiert wird. Die Aktualisierung ist möglichst automatisiert vorzunehmen.

db) Werden sensitive Daten aus nichtöffentlichen Sitzungen auf Systemen außerhalb der Verwaltung gespeichert, sind diese Daten in geeigneter Weise gegen einen unbefugten Zugriff abzusichern.

dc) Dazu ist es erforderlich, auf privaten PC Betriebssysteme zu verwenden, die eine Nutzerauthentifizierung ermöglichen und in der Lage sind, Rechtekonzepte wirkungsvoll umzusetzen.

dd) Darüber hinaus ist eine Verschlüsselung der aus dem Ratsinformationssystem übertragenen Daten anzustreben.

de) Sofern Mandatsträger ihre ehrenamtliche Tätigkeit beenden, ist sicherzustellen, dass die auf den heimischen PC gespeicherten vertraulichen Sitzungsunterlagen durch die Mandatsträger umgehend dauerhaft und unwiederbringlich gelöscht werden.

df) Wegen der damit verbundenen besonderen Risiken für die Betroffenen hat die Verarbeitung von Daten der Schutzstufe E in Ratsinformationssystemen, wie in allen vernetzten Systemen, zu unterbleiben.

IX. Veröffentlichung von personenbezogenen Daten der Mandatsträger im Internet

In die Ratsinformationssysteme oder gemeindliche Internetangebote werden vielfach auch Informationen über die Zusammensetzung der kommunalen Gremien und deren Mitglieder eingestellt. So finden sich häufig neben einem Porträtfoto Angaben über den Vor- und Zunamen des Mandatsträgers, seine Parteizugehörigkeit sowie private Adress- und Kommunikationsdaten

Diese Daten sind für ein Ratsinformationssystem grundsätzlich verwendbar. Darüber hinaus gilt, dass weitere personenbezogene Angaben über den Mandatsträger ohne dessen Einwilligung nur dann veröffentlicht werden dürfen, wenn diese Informationen der Öffentlichkeit bereits bekannt sind, so etwa aus der letzten amtlichen Wahlbekanntmachung. Für die Veröffentlichung weiterer Fotos und sonstiger, dem privaten oder beruflichen Lebensumfeld (hierzu gehören beispielsweise auch die beruflichen Kommunikationsdaten) zuzurechnender Einzelangaben bedarf es der vorherigen schriftlichen Einwilligung des Mandatsträgers.

Es wird empfohlen, die Einwilligung bereits bei Antritt des Mandats im Zuge der Verpflichtung einzuholen.