Die Landesbeauftragte für den
Datenschutz Niedersachsen

DATENSCHUTZ FÜR KOMMUNALE ABGEORDNETE

HANDREICHUNG (OKTOBER 2021)

www.lfd.niedersachsen.de

Handreichung zum Datenschutz für kommunale Abgeordnete
Oktober 2021

HERAUSGEBERIN
Die Landesbeauftragte
für den Datenschutz Niedersachsen
Prinzenstraße 5 | 30159 Hannover
Postfach 221 | 30002 Hannover
Telefon +49 (0) 511 120-4500
Telefax +49 (0) 511 120-4599
poststelle@lfd.niedersachsen.de
www.lfd.niedersachsen.de

INHALTSVERZEICHNIS

VORWORT 4

I. RATSARBEIT UND DATENSCHUTZ - FRAGEN UND ANTWORTEN 5

II. RATS- UND BÜRGERINFORMATIONSSYSTEME ... 14

III. LIVESTREAMING VON RATSSITZUNGEN 14

IV. SICHERER EINSATZ TECHNISCHER GERÄTE IN DER GREMIENARBEIT 15

V. WEITEFÜHRENDE LINKS 17

VI. AUFGABEN DER LFD NIEDERSACHSEN 17

VORWORT

Sehr geehrte Leserinnen und Leser,

am 12. September 2021 fanden in Niedersachsen die Kommunalwahlen statt. Zum Beginn der Wahlperiode am 1. November nehmen die gewählten Abgeordneten ihre Arbeit in den Kommunalparlamenten auf. Gerade wenn man ein solches Amt neu übernimmt, stellen sich zahlreiche Fragen und Herausforderungen.

Eine dieser Herausforderungen besteht darin, auf der einen Seite dem Informationsinteresse der Bürgerinnen und Bürger an der Gremienarbeit gerecht zu werden und auf der anderen Seite dabei die datenschutzrechtlichen Bestimmungen einzuhalten. Um die Mandatsträgerinnen und Mandatsträger dabei zu unterstützen, diesen Balanceakt zu meistern, habe ich diese Handreichung zusammengestellt. Sie soll ganz konkrete Fragen aus der täglichen Gremienarbeit beantworten und das allgemeine Bewusstsein für den Datenschutz schärfen.

Ich wünsche allen Leserinnen und Lesern eine informative und hoffentlich erhellende Lektüre sowie den Abgeordneten viel Erfolg bei der Wahrnehmung ihrer Aufgaben.

Barbara Thiel

Die Landesbeauftragte für den Datenschutz Niedersachsen

Hannover, im Oktober 2021

I. RATSARBEIT UND DATENSCHUTZ - FRAGEN UND ANTWORTEN

Ratsmitglieder haben in Ausübung ihrer Tätigkeit Zugang zu sehr vertraulichen Daten, die nicht für die Öffentlichkeit bestimmt sind. Personenbezogene Daten werden durch das Grundrecht auf informationelle Selbstbestimmung verfassungsrechtlich geschützt (vgl. das sogenannte „Volkszählungsurteil" des Bundesverfassungsgerichts, BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215). Dieser Schutz gilt sowohl für die personenbezogenen Daten der Bürgerinnen und Bürger als auch für die Daten der Ratsmitglieder.

Seit dem 25. Mai 2018 gilt die EU-Datenschutzgrundverordnung (DS-GVO; ABl. L 119/2016) unmittelbar in allen EU-Mitgliedsstaaten. Ein wesentlicher Grundsatz der DS-GVO ist das sogenannte Verbot mit Erlaubnisvorbehalt. Dies bedeutet, dass die Verarbeitung personenbezogener Daten nur zulässig ist, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt oder die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

Für die Verarbeitung personenbezogener Daten durch Ratsmitglieder finden neben den allgemeinen Bestimmungen der DS-GVO vor allem das Niedersächsische Datenschutzgesetz (NDSG; Nds. GVBl. 2018, 66) sowie spezialgesetzliche Regelungen wie zum Beispiel das Niedersächsische Kommunalverfassungsgesetz (NKomVG; Nds. GVBl. 2010, 576) Anwendung.

Der nachfolgende Katalog enthält Antworten auf häufig gestellte Fragen aus der täglichen Praxis der kommunalen Abgeordneten – ohne Anspruch auf Vollständigkeit.

1. Wie ist der Begriff „personenbezogene Daten" definiert?

Gemäß Art. 4 Nr. 1 DS-GVO sind dies alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (sogenannte „betroffene Person") beziehen (z.B. Name, Geburtsdatum, Familienstand, Anschrift, Foto oder Video einer Person). Solange ein Rückschluss auf eine Person möglich ist, gelten Daten als personenbezogen.

2. Was versteht man unter Datenverarbeitung?

Gemäß Art. 4 Nr. 2 DS-GVO versteht man unter Datenverarbeitung u.a. das Erheben, die Speicherung, die Offenlegung (z.B. Übermittlung) sowie das Löschen personenbezogener Daten

3. Wer ist für die Verarbeitung personenbezogener Daten verantwortlich?

Die Tätigkeit des Rates, der ein Organ der Kommune ist, wird der Kommune zugerechnet. Sofern ein Ratsmitglied personenbezogene Daten im Rahmen der Ratstätigkeit verarbeitet, wird dies dem Rat und somit der Kommune zugerechnet. Abzugrenzen hiervon ist der Fall, in dem ein Ratsmitglied offenkundig privat oder im Rahmen seiner Tätigkeit als Parteimitglied (z.B. im Rahmen des Wahlkampfs) personenbezogene Daten verarbeitet. In diesem Fall wird das Handeln nicht der Kommune zugerechnet, sondern dem Ratsmitglied als Privatperson.

4. Wie kommen Sie als Abgeordnete mit personenbezogenen Daten in Berührung?

Im Rahmen Ihrer Tätigkeit als Abgeordnete wird es immer wieder vorkommen, dass Sie Kenntnis von personenbezogenen Daten erlangen und diese möglicherweise anderweitig verarbeiten. So können zum Beispiel Sitzungsunterlagen personenbezogene Daten von Bürgerinnen und Bürgern enthalten oder es werden im Rahmen einer Gremiendiskussion personenbezogene Daten preisgegeben. Beinhalten die Sitzungsunterlagen Daten, die Rückschlüsse auf eine bestimmte Person zulassen (relevant ist dies insbesondere bei Grundstücksangelegenheiten, im Zusammenhang mit Personalangelegenheiten oder bei Vergabeentscheidungen etc.), so müssen diese Daten vor der Veröffentlichung der Unterlagen z.B. in einem Bürgerinformationssystem geschwärzt werden.

5. 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 schriftlich oder elektronisch (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.

6. Was ist unter dem Begriff der Amtsverschwiegenheit zu verstehen?

Eine 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 Tätigkeit erfahren haben und die der Geheimhaltung unterliegen.

Dies bedeutet, dass Sie verpflichtet sind, 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, Presse etc.) weiter, so kann dies in Einzelfällen eine bußgeldbewährte Ordnungswidrigkeit (§ 59 NDSG) bzw. in manchen Fällen sogar eine Straftat (§ 60 NDSG) darstellen. Die Verschwiegenheitspflicht gilt auch nach Beendigung der Abgeordnetentätigkeit.

7. Was passiert mit personenbezogenen Daten, wenn Sie diese für Ihre Mandatstätigkeit nicht mehr benötigen, weil der Vorgang abgeschlossen ist?

Personenbezogene Daten sind zu löschen, wenn die Daten für den Zweck, zu dem sie verarbeitet wurden, nicht mehr erforderlich sind und Aufbewahrungsfristen nicht entgegenstehen (Art. 17 DS-GVO). Dies ist beispielsweise der Fall, sobald der Sitzungsgegenstand abschließend behandelt worden ist.

8. Wie ist mit Sitzungsniederschriften zu verfahren?

Vor der Veröffentlichung von Verlaufs- oder Ergebnisprotokollen über öffentliche Sitzungen ist darauf zu achten, dass diese keine personenbezogenen Daten von Bürgerinnen und Bürgern enthalten. Niederschriften nicht-öffentlicher Sitzungen sind nur denjenigen Abgeordneten zuzusenden, die an der Sitzung teilgenommen haben bzw. hätten teilnehmen dürfen.

9. Dürfen Sie Sitzungsunterlagen an Dritte weitergeben?

Nein, das ist nicht zulässig. Dies betrifft auch die Mitteilung über den Inhalt entsprechender Unterlagen. Als Dritte einzustufen sind beispielsweise Familienmitglieder, Kolleginnen und Kollegen außerhalb des Rats, Bekannte, Nachbarinnen und Nachbarn sowie Mitglieder der eigenen Partei. Endet Ihr Mandat, so müssen Sie alle verbliebenen Unterlagen an die Verwaltung zurückgeben bzw. datenschutzgerecht vernichten.

Grundsätzlich sind Sie als Abgeordnete dazu verpflichtet, alle Unterlagen, die personenbezogene Daten enthalten, vor dem Zugriff durch Dritte zu schützen. Sitzungsunterlagen sind ausschließlich für den Verwaltungsgebrauch bzw. für Ihre Arbeit als Abgeordnete oder Abgeordneter bestimmt.

10. 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 wieder zurück. Fällt ein Ausschussmitglied derartig kurzfristig aus, dass es die Sitzungsunterlagen persönlich nicht mehr rechtzeitig an seine Vertretung weitergeben kann, so kann sich diese die Unterlagen bei ihrer Fraktion besorgen. Der Fraktion steht immer ein kompletter Satz der jeweiligen Sitzungsunterlagen zur Verfügung.

Soweit in Ihrer Kommune ein Ratsinformationssystem verwendet wird, können den Vertreterinnen und Vertretern im Vertretungsfall auch entsprechende Zugriffsrechte eingeräumt werden.

11. Dürfen Daten von Abgeordneten durch die Verwaltung bekannt gegeben werden?

Beabsichtigt die Kommune die Veröffentlichung personenbezogener Daten von kommunalen Abgeordneten, die über Vor- und Zuname hinausgehen, so bedarf es der vorherigen Einwilligung der betroffenen Abgeordneten. Das ist auch der Fall, wenn die Daten anlässlich der Kommunalwahl bereits öffentlich bekannt gemacht worden sind.

12. Haben Sie die Möglichkeit, Auskunft über die über Sie gespeicherten Daten bei der Verwaltung zu bekommen?

Art. 15 DS-GVO regelt das Recht auf Auskunft über die personenbezogenen Daten der um Auskunft ersuchenden Person, die eine verantwortliche Stelle verarbeitet. Dieses Recht steht auch den Abgeordneten gegenüber der Verwaltung zu. Die Daten verarbeitende Stelle muss Ihnen auf Antrag Auskünfte erteilen über die zu Ihrer Person gespeicherten Daten. Dieser Auskunftsanspruch ist ein wesentlicher Bestandteil Ihres Rechts auf informationelle Selbstbestimmung.

13. Kann Ihnen die Auskunft verweigert werden?

§ 9 NDSG regelt für bestimmte Ausnahmetatbestände Beschränkungen des Rechts auf Auskunft. Die Auskunft kann demnach u.a. dann verweigert werden, wenn die Auskunftserteilung die öffentliche Sicherheit gefährden würde oder dem Wohl des Bundes bzw. der Länder Nachteile entstünden. Die Auskunft darf zudem verweigert werden, wenn die Auskunft dazu führen würde, dass ein Sachverhalt aufgedeckt würde, der nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten einer anderen Person geheim zu halten ist. Ein weiterer Hinderungsgrund der Auskunftserteilung besteht dann, wenn dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten erforderlich ist.

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. Das heißt, es dürfen nur die Daten aus den Bewerbungsunterlagen verarbeitet und an das für die Entscheidung zuständige Gremium weitergeleitet werden, die für die jeweilige Entscheidungsfindung erforderlich sind.

Maßgeblich hierfür ist dabei das in der Ausschreibung genannte Anforderungsprofil für den zu besetzenden Arbeitsplatz/Dienstposten unter Berücksichtigung der Kriterien der Bestenauslese (Art. 33 Abs. 2 des Grundgesetzes).

15. Sind für die Änderung des Stellenplans personenbezogene Daten zu erheben?

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

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?

Nein, dies ist unzulässig. Auch wenn es sich bei betriebsbezogenen Daten nicht immer um personenbezogene Daten handelt, sind diese Daten regelmäßig durch anderweitige Rechtsvorschriften geschützt. So ist in der Abgabenordnung (AO) das Steuergeheimnis besonders geschützt (§ 30 AO). Danach ist die Weitergabe der Daten im vorliegenden Fall u. a. nur dann möglich, wenn diese Daten für ein Verwaltungsverfahren benötigt werden. Allenfalls könnten anonymisierte Daten, wie z. B. Zahlen über das Gesamtaufkommen an Gewerbesteuer der vergangenen Jahre, weitergegeben werden (vgl. auch § 4 Abs. 2 Nr. 2 des Niedersächsischen Pressegesetzes).

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, dies ist nicht zulässig, da diese Daten dem Sozialgeheimnis gemäß § 35 SGB I i.V.m.§§ 67 ff. SGB X unterliegen. Die Daten dürfen nur mit vorheriger Einwilligung der betroffenen Personen weitergegeben werden, da sie nicht zu dem Zweck verwendet werden sollen, für den sie ursprünglich 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 Personen zu informieren, können Sie über die örtliche Presse, einen Informationsstand oder Flugblätter erreichen.

18. Aufgrund von wiederholt aufgetretenen Sachbeschädigungen an öffentlichen Gebäuden möchte die Verwaltung eine Videoüberwachungsanlage installieren. Darf sie das?

Öffentlich zugängliche Bereiche dürfen unter den Voraussetzungen des § 14 NDSG durch Bildübertragung (Videoüberwachung) beobachtet werden. Bevor die Überwachungstechnik aber eingesetzt wird, ist – neben einer eingehenden Prüfung der Geeignetheit und Erforderlichkeit sowie einer Abwägung mit möglichen widerstreitenden Interessen – eine Vielzahl von Formvorschriften zu beachten.

So muss z. B. vor dem Einsatz einer systematischen und umfangreichen Videoüberwachung regelmäßig eine sogenannte Datenschutz-Folgenabschätzung durchgeführt werden (Art. 35 Abs. 1 DS-GVO). 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 und -ende.

19. Dürfen personenbezogene Daten im Rahmen von Bauleitverfahren veröffentlicht werden?

Im Rahmen der Bauleitplanung können während der Beteiligung der Öffentlichkeit Stellungnahmen abgegeben werden. Diese werden bei der weiteren Beratung der Bebauungspläne von den zuständigen kommunalen Gremien in die Entscheidung miteinbezogen. Viele Kommunen veröffentlichen die eingegangenen Stellungnahmen über ihre Webseite. Dabei ist jedoch zu berücksichtigen, dass weder die baurechtlichen Vorschriften noch die allgemeinen datenschutzrechtlichen Bestimmungen die Offenlegung von personenbezogenen Daten zulassen. Vor diesem Hintergrund müssen die Kommunen sicherstellen, dass bei der Veröffentlichung der Stellungnahmen kein Personenbezug mehr vorhanden ist. Dies setzt voraus, dass sämtliche Daten, die Rückschlüsse auf eine bestimmte Person zulassen (z. B. Vorname, Name, Anschrift, Unterschrift) geschwärzt werden, bevor eingereichte Dokumente über die Webseite für die Allgemeinheit zugänglich gemacht werden.

20. Im Zuge des Kommunalwahlkampfes möchten Sie sich als Kandidatin bzw. Kandidat für die Kommunalwahl personenbezogene Daten der Erstwählerinnen und Erstwähler in Ihrer Kommune von der Verwaltung geben lassen. Dürfen Sie das?

Gemäß § 50 Abs. 1 Bundesmeldegesetz (BMG) darf die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene in den sechs einer Wahl oder Abstimmung vorangehenden Monaten Auskunft aus dem Melderegister über die in § 44 Absatz 1 Satz 1 BMG 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 ist bzw. sind, entsprechende Daten von der 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 nachfolgenden Daten dürfen gemäß § 44 Abs. 1 Satz 1 BMG von der Meldebehörde übermittelt werden:

- Familienname,
- Vornamen,
- Doktorgrad und die
- derzeitigen Anschriften.

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 Personen haben gemäß § 50 Abs. 5 BMG das Recht, einer Übermittlung ihrer Daten an Parteien, Wählergruppen und andere Trägerinnen und Träger von Wahlvorschlägen zu widersprechen. Auf diese Möglichkeit ist bei der melderechtlichen Anmeldung und einmal jährlich durch öffentliche Bekanntmachung hinzuweisen. Diese Meldedaten werden Ihnen nicht übermittelt.

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.

21. Können Sie außerhalb der Sechsmonatsfrist vor Wahlen mit Hilfe der sogenannten „Gruppenauskunft" gemäß § 46 BMG Daten aus dem Melderegister bekommen?

Nein, dies ist nicht zulässig. 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.

22. Dürfen Meldedaten im Zusammenhang mit Alters- bzw. Ehejubiläen verarbeitet werden?

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 über die nachfolgenden Daten erteilen:

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

Unter Altersjubiläen versteht man den 70. Geburtstag, jeden fünften weiteren Geburtstag sowie ab dem 100. Geburtstag jeden folgenden. Zu den Ehejubiläen zählen das 50. sowie jedes folgende.

Die betroffenen Personen haben gemäß § 50 Abs. 5 BMG das Recht, dieser Übermittlung zu widersprechen. Auf diese Möglichkeit ist bei der melderechtlichen Anmeldung und einmal jährlich durch öffentliche Bekanntmachung hinzuweisen.

23. Dürfen Sie auch weitergehende Informationen über einzelne Personen einholen?

Die sogenannte erweiterte Melderegisterauskunft gemäß § 45 Abs. 1 BMG ist nur an Personen zulässig, die ein berechtigtes Interesse glaubhaft machen können. 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 zu einer bestimmten Person die nachfolgenden Daten 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.

24. Wer kann Ihnen bei Fragen zum Datenschutz helfen?

Jede öffentliche Stelle und damit auch jede Kommune hat gemäß Art. 37 Abs. 1 Buchstabe a) DS-GVO eine bzw. einen Datenschutzbeauftragte(n) (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 übertragen werden. Der bzw. dem DSB obliegen gemäß Art. 39 Abs. 1 DS-GVO u. a. folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen, seiner Auftragsverarbeiter sowie der mit der Verarbeitung personenbezogener Daten befassten Mitarbeiterinnen und Mitarbeiter
- Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften
- Zusammenarbeit mit der Datenschutzaufsichtsbehörde

Eine weitere wichtige Aufgabe der bzw. des DSB besteht darin, dass sie bzw. er auf der örtlichen Ebene als Ansprechpartnerin bzw. Ansprechpartner für Fragen des Datenschutzes zur Verfügung steht. Artikel 37 Abs. 7 DS-GVO 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 bzw. den DSB wenden. Dasselbe gilt für die Bediensteten der Behörde sowie für Ratsmitglieder.

25. Dürfen Sie während einer Ratssitzung gefilmt werden?

Grundsätzlich dürfen öffentliche Sitzungen des Rates per Video übertragen werden. Voraussetzung ist, dass die Hauptsatzung der Kommune eine entsprechende Regelung enthält. Allerdings haben Sie als Mandatsträgerinnen und Mandatsträger auch die Möglichkeit zu verlangen, dass Ihre Redebeiträge nicht im Internet bzw. im Fernsehen übertragen werden (detailliertere Ausführungen unter „III. Livestreaming von Ratssitzungen").

26. Dürfen Sie Daten zur Ratsarbeit auf Ihrem eigenen Handy oder Tablet verarbeiten?

Grundsätzlich wird davon aus Gründen der Datensicherheit abgeraten. Erfahrungsgemäß sind nur wenige Nutzerinnen und Nutzer mobiler Endgeräte selbst in der Lage, diese hinreichend sicher zu administrieren. Der Einsatz privater Endgeräte (sog. Bring Your Own Device, BYOD-Ansatz) sollte daher aus datenschutzrechtlicher Sicht nur erfolgen, wenn die privaten Endgeräte lediglich als Web-Endgerät genutzt werden und gewährleistet ist, dass die eigentliche Anwendung und Datenverarbeitung (Speicherung, Transformation, Nutzersteuerung durch Rechte-Rollen-Konzepte usw.) ausschließlich auf einem gesicherten Server der Kommune und nicht lokal auf dem mobilen Endgerät erfolgt. Die Nutzung des privaten Endgerätes würde somit lediglich in der reduzierten Funktion ähnlich einem Terminal für die Ein- und Ausgabe genutzt werden (detaillierte Ausführungen unter „IV. Sicherer Einsatz technischer Geräte in der Gremienarbeit").

II. RATS- UND BÜRGER-INFORMATIONSSYSTEME

Tagesordnungen, Vorlagen und amtliche Niederschriften öffentlicher Sitzungen werden im Rahmen der gesetzlichen Vorgaben von den Kommunen veröffentlicht. Im Rahmen der Abwicklung des Sitzungsdienstes arbeiten viele Kommunen mit Rats- und Bürgerinformationssystemen. Die Ratsinformationssysteme sind geschlossene Systeme, auf welche nur die Rats- bzw. Ausschussmitglieder Zugriff haben.

Ihre Nutzung ist daher aus datenschutzrechtlicher Sicht unproblematisch. Die Bürgerinformationssysteme hingegen sind öffentliche Systeme, auf die jedermann online zugreifen kann. Die dort eingestellten Unterlagen dürfen deshalb keine personenbezogenen Daten enthalten. Erforderlichenfalls sind die Unterlagen zu anonymisieren.

III. LIVESTREAMING VON RATSSITZUNGEN

Einige Kommunen möchten öffentliche Sitzungen im Internet über ihre Webseite (z.B. Live-Streaming) oder auf regionalen TV-Sendern übertragen lassen. Im Zuge dieser Übertragungen werden personenbezogene Daten verarbeitet. In Niedersachsen findet sich die Rechtsgrundlage für die Übertragung von Bild- und Tonaufnahmen der Sitzung der Vertretung in § 64 Absatz 2 Satz 2 NKomVG.

Demnach sind Bild- und Tonaufnahmen von Mitgliedern der Vertretung mit dem Ziel der Berichterstattung zulässig, wenn die Hauptsatzung der Kommune eine entsprechende Regelung enthält. Aus datenschutzrechtlicher Sicht ist insbesondere zu beachten, dass keine Aufnahmen von Personen gemacht werden, die nicht Mitglieder der Vertretung sind, also zum Beispiel von Zuschauerinnen und Zuschauern der Ratssitzungen. Von diesen Personen muss immer vor Beginn der Bild- und/oder Tonaufnahmen eine Einwilligung eingeholt werden. Auch die Mandatsträgerinnen und Mandatsträger haben die Möglichkeit zu verlangen, dass ihre Redebeiträge nicht im Internet bzw. im Fernsehen übertragen werden (§ 64 Abs. 2 Satz 3 NKomVG).

IV. SICHERER EINSATZ TECHNISCHER GERÄTE IN DER GREMIENARBEIT

Personenbezogene Daten müssen u. a. nach den Grundsätzen des Art. 5 Abs. 1 lit. f) sowie nach Art. 24, 25 und 32 DS-GVO in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Die Gewährleistung von Datensicherheit ist ein zentrales Prinzip des Datenschutzes und umfasst die Summe aller technischen und organisatorischen Sicherungsmaßnahmen (TOM), die erforderlich sind, um eine den Datenschutznormen entsprechende Datenverarbeitung sicher zu stellen und damit die Rechte und Freiheiten natürlicher Personen angemessen zu schützen. Es gilt, unbefugter oder unrechtmäßiger Verarbeitung und unbeabsichtigtem Verlust sowie unbeabsichtigter Zerstörung oder Schädigung vorzubeugen.

Kommen in der kommunalen Gremienarbeit technische Geräte zur Verarbeitung personenbezogener Daten zum Einsatz, sind demnach die erforderlichen angemessenen TOM zur Datensicherheit zu treffen. Dies ist Aufgabe des Verantwortlichen (und ggf. eines Auftragsverarbeiters), nicht die des Herstellers der Geräte, Systeme und Anwendungsprogramme. Die TOM trifft der Verantwortliche sowohl, wenn er die Mittel für die Verarbeitung festlegt als auch zum Zeitpunkt der eigentlichen Verarbeitung (Datenschutz durch Technikgestaltung, Art. 25 Abs. 1 DS-GVO). Zudem trifft er geeignete TOM, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind (Datenschutz durch datenschutzfreundliche Voreinstellungen, Art. 25 Abs. 2 DS-GVO).

Bei der Auswahl der TOM ist zu beachten, dass dies unter Berücksichtigung des Risikos, also der Eintrittswahrscheinlichkeit und Schadenshöhe für die Rechte und Freiheiten natürlicher Personen, des Standes der Technik und der Implementierungskosten sowie der Art, Umstände und des Zwecks der Datenverarbeitung geschieht. Die Maßnahmen müssen wirksam und je nach den Abwägungsergebnissen angemessen sein. Dieser Schritt dient dazu, sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den datenschutzrechtlichen Bestimmungen erfolgt. Schließlich müssen nach der Bestimmung der Maßnahmen das Restrisiko bewertet und die Maßnahmen ggf. konsolidiert werden.

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

Soweit mobile Endgeräte (z. B. Notebooks, Tablets oder Smartphones) für die Gremienarbeit zum Einsatz kommen, birgt dies je nach Netzanbindung, Betriebssystem und Anwendungsumgebung zusätzliche spezifische Gefährdungsaspekte wie z. B. zusätzliche Sicherheitslücken oder technische Schwachstellen. Beim Einsatz dienstlicher Geräte müssen diese ebenso hinsichtlich ihrer Risikopotenziale bewertet werden, um die angemessenen wirksamen TOM festzulegen und umzusetzen.

Einen wertvollen grundlegenden Beitrag zur Datensicherheit können Kommunen leisten, indem sie den Abgeordneten sichere und datenschutzkonform ausgestaltete Systeme zur Verfügung stellen, die mittels einer zentral administrierten und gemanagten Einbindung der Geräte unter IT-fachlicher Kontrolle stehen. Die Bereitstellung und Administration der mobilen Endgeräte obliegen damit der Kommune. Zusätzlich ist eine

Informationssicherheitsrichtlinie einschließlich der Datenschutzmaßnahmen und ein Datenschutzkonzept zur Durchsetzung der TOM erforderlich, die jeweils wegen der technischen Weiterentwicklung zyklisch fortzuschreiben sind.

Bedingt durch die Vielfalt möglicher Betriebssysteme, die Notwendigkeit des Vorhaltens und der aktuellen Konfiguration komplexerer Sicherheitsanwendungen (Firewall, Virenschutz, Verschlüsselung etc.) sowie ständig wechselnder und weiterentwickelter Angriffsszenarien auf Soft- und Hardwareschwachstellen sind der Erfahrung nach nur wenige Nutzerinnen und Nutzer mobiler Endgeräte selbst in der Lage, diese hinreichend sicher zu administrieren. Der Einsatz privater Endgeräte (sog. Bring Your Own Device, BYOD-Ansatz) sollte daher aus datenschutzrechtlicher Sicht nur erfolgen, wenn die privaten Endgeräte lediglich als Web-Endgerät genutzt werden und gewährleistet ist, dass die eigentliche Anwendung und Datenverarbeitung (Speicherung, Transformation, Nutzersteuerung durch Rechte-Rollen-Konzepte usw.) ausschließlich auf einem gesicherten Server der Kommune (oder auf dem Server eines Auftragsverarbeiters i. S. v. Art. 4 Nr. 8 DS-GVO) und nicht lokal auf dem mobilen Endgerät erfolgt. Die Nutzung des privaten Endgerätes würde somit lediglich in der reduzierten Funktion ähnlich einem Terminal für die Ein- und Ausgabe genutzt werden.

Soweit Abgeordnete für ihre Gremienarbeit vertrauliche Daten auf einem privaten Endgerät verarbeiten, geht die Verantwortung für deren Sicherheit und Integrität auf die jeweiligen Abgeordneten über. Die Abgeordneten wären dann selbst in der Pflicht, die erforderlichen Maßnahmen zur Datensicherheit zu treffen.

Dieses Szenario ist jedoch angesichts der genannten Risikopotenziale ausdrücklich nicht empfehlenswert.

V. WEITERFÜHRENDE LINKS

Informationen der LfD Niedersachsen zum Datenschutz in Kommunen

FAQ zu den Regelungen der DS-GVO in Kommunen

Handreichung zur Anfertigung und Veröffentlichung von Personenfotografien im öffentlichen Bereich

Übersicht der aktuell geltenden Datenschutzgesetze

Niedersächsisches Datenschutzgesetz

VI. AUFGABEN DER LANDESBEAUFTRAGTEN FÜR DEN DATENSCHUTZ NIEDERSACHSEN

Zu den Aufgaben der vom Landtag gewählten Landesbeauftragten für den Datenschutz gehört es, datenschutzrechtliche Interessen von Bürgerinnen und Bürgern gegenüber öffentlichen Stellen und Unternehmen zu vertreten sowie die Öffentlichkeit für die Belange des Datenschutzes zu sensibilisieren. Eine detaillierte Auflistung ihrer gesetzlich festgeschriebenen Aufgaben findet sich in Artikel 57 der Datenschutz-Grundverordnung. Danach müssen die Aufsichtsbehörden unter anderem:

- die Anwendung der DS-GVO überwachen und durchsetzen;
- die Öffentlichkeit für die Risiken und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten sensibilisieren;
- Parlamente und Regierungen beraten;
- Verantwortliche und Auftragsverarbeiter für ihre Pflichten sensibilisieren;
- sowie Beschwerden von Betroffenen bearbeiten.

Prinzenstraße 5 | 30159 Hannover
Postfach 221 | 30002 Hannover

Telefon +49 (0) 511 120-4500
Telefax +49 (0) 511 120-4511

poststelle@lfd.niedersachsen.de